



The Directors' Toolkit

Your guide to good governance
Edition 7



• FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Foreword

It is never easy to pick the right time to release the latest edition of *The Directors' Toolkit* because a new governance change is always around the corner. We typically try to align release with changes to the ASX Governance Council's updates to the Corporate Governance Principles and Recommendations (ASX Principles and Recommendations), however, given the ASX's decision not to proceed with the proposed 5th Edition of the latter, we have decided to launch our Toolkit update regardless.

Where the previously proposed 5th Edition included significant changes to a specific recommendation, we have included this for reference as we thought you may enjoy understanding the ASX's proposed direction with the new Edition even if this may change in the next iteration of the 5th Edition. We will of course update the Toolkit when the 5th Edition is issued.

As governance continues to evolve at a rapid pace, this Toolkit update reflects on the significant developments that have emerged since our last release. Notably, the rise of artificial intelligence (AI) has shifted from a distant concept to a central consideration in boardroom discussions. This shift brings both opportunities for efficiency and effectiveness, as well as new challenges in risk and oversight that demand thoughtful governance responses.

The governance environment has also continued to focus on how to achieve better diversity in the boardroom so as to reduce groupthink and better understand, and give regard to, key stakeholders. These were some of the proposed changes to the ASX Principles

and Recommendations and we anticipate that the future iteration of the 5th Edition will incorporate these concepts in some way. The proposed changes sparked meaningful dialogue and underscored the complexities in achieving diversity beyond gender. The debate also enabled reflection and challenge on what should stay in the boardroom and what should be publicly reported.

In addition to these thematic shifts, the Toolkit incorporates insights from recent governance failures as well as legislative changes. Our aim is to distill these developments into practical guidance that helps directors navigate key aspects of the regulatory landscape. Feedback from directors consistently highlights the burden of keeping across all these changes and their role in oversight. It is our hope that this resource provides clarity and support in managing those demands.

We trust that this updated Toolkit will serve as a valuable companion in your governance journey.



Caron Sugars
Lead Partner,
Board Advisory Services

The information contained herein is of a general nature only, and is not intended to be comprehensive. It is not legal advice, and should not be relied upon as such. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. Accordingly, KPMG makes no warranties or representations regarding any of the content. No one should act on such information without appropriate professional advice after a thorough examination of their particular situation and circumstances. KPMG excludes, to the maximum extent permitted by law, any liability which may arise in relation to the content.

The Role of Boards and Directors



FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

1. Directors' Legal Duties

Company directors have significant legal responsibilities. It is critical to understand these duties, maintain compliance and keep up to date on any relevant changes to legislation.

In this chapter

- Constitution
- ASX listing requirements
- Key duties and responsibilities
- Acting in good faith
- Use of position and information
- Care and diligence
- Business judgement rule
- Other legal obligations
- Directors' indemnities and insurance
- Conflict and disclosure of interests
- Related party transactions
- Insolvent trading and safe harbour
- Continuous disclosure
- Insider trading
- Record keeping
- Share trading by directors
- Resignation
- Enforcement, penalties and remedies

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Do I have a good working knowledge of the constitution, laws, regulations and the Australian Securities Exchange (ASX) Listing Rules relevant to the company?
2. Do the directors have access to company records, reports from management and updates about material changes to the relevant laws and regulations? Are they provided quality information in a timely manner sufficient to discharge their duties?
3. Has the board adequately considered its responsibilities under relevant WHS legislation and other legislation relevant to the company and its industry?
4. Does the company secretary monitor compliance with the company's constitution or the 'replaceable rules' (whichever applies)?
5. Do I understand the scope and limitations of the directors' and officers' liability insurance policy?
6. Is the board immediately advised of queries received from the ASX, the Australian Securities and Investments Commission (ASIC) or other regulators?
7. Is there a system in place for regulatory breaches to be reported to the directors?
8. Am I fully aware of my duties and responsibilities regarding conflicts of interest? Are directors' interests properly disclosed in the financial statements and directors' report?
9. Is there an effective procedure for identifying and disclosing related party transactions?
10. Does the company have effective monitoring mechanisms in place to ensure that market sensitive information is not leaked to the public before it is provided to the ASX?
11. Am I fully aware of my duties and responsibilities regarding solvency and the safe harbour provisions?
12. Am I fully aware of my responsibilities under continuous disclosure requirements?
13. If I am a director of a superannuation trustee (and RSE Licensee) do I have a good working knowledge of the additional duties and obligations placed on directors by the trust deed and the *Superannuation Industry (Supervision) Act 1993* (Cth)?

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The company's constitution is never, or rarely, referred to in board discussions/documentation.
- Certain directors are perceived to have conflicts of interest (for example, they have close personal ties with a major supplier or contractor).
- The directors fail to act in the best interests of the company as a whole (e.g. by having undue regard to the interests of a special interest group or major shareholder).
- A director lets price sensitive information slip at a social gathering or on social media.
- The board ignores a solvency problem or does not act accordingly to seek further information (accounting or otherwise) or implement a plan.
- There are concerns about certain directors or officers trading in company securities immediately before public announcements and/or there is a lack of awareness in relation to the company's securities trading policy.
- Insufficient time is paid to major decisions/proposals or the annual financial statements.
- Directors have difficulty accessing company information in a timely manner.
- The board does not receive updates on changes to relevant WHS legislation and other legislation relevant to the company and its industry.
- No reporting on regulatory compliance and breaches are provided to the directors.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Company directors' responsibilities are derived from the *Corporations Act 2001* (Cth) (the Corporations Act), the company's constitution, relevant common law principles and a range of other legislative and regulatory regimes. This includes trade practices law, workplace health and safety (WHS) obligations, environmental obligations, privacy and equal opportunity requirements. Company directors should be familiar with the material laws, regulations and rules relevant to the entities that they govern.

Whilst this chapter contains an overview of some of the key duties, it is not intended as a comprehensive summation of all company officer and director duties. Directors should always seek legal advice if they are uncertain about their legal position.

Circumstances can arise where directors of a company can be held personally responsible for breaching certain laws, even when they did not specifically authorise such a breach.

Directors have the power to control the management of a company's property and affairs and, as such, are subject to special duties and responsibilities, including among others:

- a duty to act with due care, skill and diligence
- a duty to act in good faith in the best interests of the company and for a proper purpose
- a duty to avoid conflicts of interest
- a duty not to misuse position or information obtained in their capacity as a director
- a duty to prevent the company from trading while insolvent
- a duty of skill, competence and diligence in the understanding of the financial report.¹

Directors need to be vigilant to ensure that they do not expose themselves to civil or criminal liabilities by failing to properly discharge their legal duties. In practice, directors should take particular care when:

- considering whether or not the company should enter into a related party transaction
- considering if they have sufficient information (including independent expert advice) and reviewing that information when making decisions
- a company is at risk of trading whilst insolvent
- a company is involved in a takeover, either as an offeror or offeree
- a company raises money from shareholders or the general public by issuing shares or other securities.

As evidenced in the APRA CBA report,² individual directors should request further information from the company's management and/or seek their own independent legal advice if they have misgivings about a decision contemplated or taken by their board, or actions of the company's management.

In addition to their individual legal duties, the key responsibilities of the board include:

- monitoring the performance and risk management of the company
- setting, testing and improving company strategy
- setting the company's risk appetite/profile
- appointing, assessing and, where necessary, removing the CEO
- approving major capital decisions (above CEO delegation limits) including acquisitions, investments and divestments
- approving annual budgets and funding decisions.

¹ ASIC Information Sheet 183 <https://www.asic.gov.au/regulatory-resources/financial-reporting-and-audit/directors-and-financial-reporting/>

² APRA Prudential Inquiry into the Commonwealth Bank of Australia Report (April 2018) https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The role of the board as conduct and cultural leaders of the company is crucial and when issues arise it seems that the board's role in setting that tone from the top is commonly where the spotlight shines. Indeed it appears that trust is declining and the 2025 Edelman Trust Barometer shows that community trust in Australian business has declined year on year (68 per cent of those surveyed described distrust, up 12 points from 2024). In addition, 68 per cent of respondents indicated a belief that business leaders deliberately mislead them.³

As stated in the APRA CBA report,⁴ conduct risk management goes beyond what is strictly allowed under law and regulation ('can we do it?') to consider whether an action is appropriate or ethical ('should we do it?').⁵ The principle of 'Should I do this? What is the right thing to do?' is also echoed in the Hayne Royal Commission⁶ and 'Principle 3: Instil a culture of acting lawfully, ethically and responsibly' of the ASX Corporate Governance Principles and Recommendations.

Refer to [Chapter 22 Culture and Conduct](#) for more information.

Restrictions on being a director

A person cannot be a director without court consent if the individual:

- is an undischarged bankrupt
- is subject to a personal insolvency agreement or an arrangement under Part X of the *Bankruptcy Act 1966* (Bankruptcy Act) that has not been fully complied with

³ Refer to Edelman Trust Barometer 2025 <https://www.edelman.com.au/trust/2025/trust-barometer>

⁴ APRA Prudential Inquiry into The Commonwealth Bank Of Australia report (April 2018) https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf.

⁵ Ibid

⁶ Refer to Section 1.2 of Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry Final Report Volume 1 <https://www.royalcommission.gov.au/system/files/2020-09/frsc-volume-1-final-report.pdf>

- has been convicted of certain offences, including under the Corporations Act, such as a breach of duties as a director or insolvent trading. If an individual has been convicted of one of these offences, he/she must not manage a company within five years of the conviction. If imprisoned for one of these offences, the individual must not manage a company within five years after release from prison.⁷

CONSTITUTION

The power to control the affairs of the company is typically vested in the directors by the company's constitution or, where the company does not have a constitution or the constitution does not so provide, by the 'replaceable rules' of the Corporations Act.⁸

The provisions of the constitution are a key component of a company's governance framework. Directors should be familiar with the constitution and take the necessary steps to ensure it is understood, complied with and that it provides the appropriate framework for the operation of the company.

ASX LISTING REQUIREMENTS

Companies and directors of companies listed on the ASX must comply with the Listing Rules. The Listing Rules are additional obligations imposed only on listed companies, and govern the admission of companies to the ASX's 'Official List', the quotation of companies' securities, continuous disclosure obligations, directors' disclosures, suspension of securities from quotation and the removal of companies from the Official List. The Listing Rules are contractually binding between each listed company and the ASX and are enforceable against listed companies and their associates under the Corporations Act.⁹

⁷ Refer to Sections 201B and 206B of The Corporations Act 2001 and ASIC Bankruptcy and personal insolvency agreements <https://www.asic.gov.au/regulatory-resources/insolvency/insolvency-for-directors/bankruptcy-and-personal-insolvency-agreements> ASIC Information Sheet 79 <https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/your-company-and-the-law/>

⁸ Corporations Act 2001, Sections 135, 136 and 198A.

⁹ Corporations Act 2001, Sections 793C and 1101B.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Most notably, the continuous disclosure requirements under the Listing Rules are also enforceable under the Corporations Act.¹⁰ Refer to the 'Introduction to the Listing Rules'¹¹ to see the principles upon which they are based.

The ASX Corporate Governance Principles and Recommendations (Corporate Governance Principles) include a range of expected processes, disclosures and practices that listed companies apply to their organisations. Whilst not mandatory, these principles adopt an 'if not, why not' approach to reporting against the Recommendations, whereby organisations are required to report on the process in place regarding governance frameworks, assurance and risk management (as may be applicable) with respect to each Recommendation. Where processes or frameworks are not in place with respect to a particular Recommendation, then organisations are required to explain the reason for the omission, placing an onus on directors to be more transparent to shareholders across a range of governance matters. In particular, Recommendations 3.1, 3.3 and 3.4, are 'directed to setting 'the tone from the top' and ensure that the board is provided with the information it needs to monitor the culture of the organisation.¹²

Non-listed entities

Many non-listed entities choose to adopt the corporate governance guidance developed by the ASX as a means of ensuring that they align with better practice.

Registered charities (not-for-profit) organisations are not required to meet all of the reporting obligations of the Corporations Act. Registered charities are subject to the requirements of the Australian Charities and Not-for-profits Commission (ACNC). Refer to [Chapter 4 Not-For-Profit organisations](#) for more information.

¹⁰ Corporations Act, Section 674.

¹¹ ASX, The Listing Rules, <https://www.asx.com.au/documents/rules/introduction.pdf>

¹² Refer to ASX Corporate Governance Principles and Recommendations, February 2019 <https://www.asx.com.au/documents/regulation/cgc-principles-and-recommendations-fourth-edn.pdf>

Government entities are not required to meet the requirements of the Corporations Act, being instead subject to the requirements of the entity's Enabling Act. Refer to [Chapter 3 Government](#) for more information regarding government entities.

KEY DUTIES AND RESPONSIBILITIES

Whether a director of a listed, private, not-for-profit or government entity, a director's key duties are their fiduciary duties, whereby directors are expected:

- to act with due care and skill and in good faith
- to exercise power for a proper purpose, and
- avoid conflicts of interest.

In addition, the key statutory duties under the Corporations Act are that directors must:

- act with care and diligence
- act in good faith, in the best interests of the corporation, and for a proper purpose, and
- not use position or information obtained through their position to gain an advantage for themselves or others, or cause detriment to the company.¹³

The law provides that a director's duty is owed to 'the company', and the courts have typically characterised the company as being the sum of the shareholders. Whilst directors' legal duties are narrowly defined in this sense, there is a growing public expectation that directors should play an active role in 'instilling a culture of acting lawfully, ethically and responsibly' by taking account of the interests of broader stakeholder groups. Indeed, it appears from the consultation draft for a proposed fifth edition of the Corporate Governance Principles¹⁴ that in the next iteration Principle 3 will extend further to be explicit regarding how this culture extends to 'dealings with external stakeholders, to create long-term sustainable value'.

¹³ Corporations Act 2001, Sections 180-183.

¹⁴ ASX, Consultation Draft for a proposed fifth edition of the Principles and Recommendations, <https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/corporate-governance-principles-and-recommendations-consultation-draft.pdf>

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

However, any decisions must ultimately be in the best interests of the company's shareholders collectively for directors to discharge their duties under the Corporations Act (as set out below).

The Corporations Act outlines the duties and liabilities of directors and other 'officers'¹⁵ of a company. The duties apply not only to validly appointed directors (including alternate directors), but also to 'de facto directors' and 'shadow directors'.

ACTING IN GOOD FAITH

Directors and other officers of a company are under a statutory and common law duty to act in good faith and in the best interests of the company as a whole and for a proper purpose.¹⁶ This duty recognises that a director's primary responsibility is to the company and that this responsibility must ordinarily take precedence over the personal interests of the director or the interests of a third party. The duty to act in good faith is a broad duty that requires directors to:

- exercise their powers only for proper corporate purposes
- avoid actual, potential and perceived conflicts of interest
- account to the company for business opportunities that arise.

USE OF POSITION AND INFORMATION

Directors and other officers and employees of a company must not improperly use their position or information they receive to gain an advantage for themselves or someone else, or to cause a detriment to the company.¹⁷

This duty would, for example, prohibit a director from obtaining a personal benefit through the misuse of the company's client or supplier list.

An offence is committed under both statute and common law if it can be shown that the conduct was undertaken with the intention of gaining an advantage. It is not necessary to establish that the advantage was actually obtained.

CARE AND DILIGENCE

Directors and other officers must exercise their duties with the degree of care and diligence that a reasonable person would exercise if they were a director or officer in the circumstances of the company and occupied the same responsibilities within the company as the director.¹⁸ Matters to consider include the director's position and responsibilities within the company, the company's circumstances and any special expertise of the director.¹⁹

BUSINESS JUDGEMENT RULE

A director who makes a business judgement is taken to satisfy their duty of care and diligence in respect of the judgement if they:

- make the business judgement in good faith and for a proper purpose (a 'business judgement' being any decision to take or not take action in respect of a matter relevant to the operations of the corporation)²⁰
- do not have a material personal interest in the subject matter of the judgement
- inform themselves about the subject matter of the judgement to the extent they reasonably believe to be appropriate
- rationally believe that the judgement is in the best interests of the company.²¹

¹⁸ Section 180 Corporations Act 2001.

¹⁹ For case law guidance on the standard required of directors to effectively discharge the duty of care and diligence, see *Daniels v Anderson* (1995) 37 NSWLR 438; 118 FLR 248; 16 ACSR 607; 13 ACLC 614 (the AWA case), *ASIC v Adler* (2002) 168 FLR 253; 41 ACSR 72; 20 ACLC 576; [2002] NSWSC 171 at [372].

²⁰ Corporations Act 2001, Section 180(3).

²¹ Corporations Act 2001, Section 180(2).

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The business judgement rule does not protect a cavalier attitude to business risk. Directors are expected to make informed business judgements and they must have a rational belief that their decisions are in the best interests of the company. The director's belief that the judgement is in the best interests of the company is a rational one, unless the belief is one that no reasonable person in their position would hold. This means that directors should exercise their powers and discharge their duties with the degree of care and diligence expected of any reasonable person in their position.

Directors making a business judgement are regarded as having discharged their duty of care and diligence under the Corporations Act and their equivalent duties at common law or in equity (including the duty of care that arises under the common law principles governing the liability for negligence). The business judgement rule only applies as a defence to section 180(1) of the Corporations Act.

Courts do not, in general, second-guess the business judgement of directors based on the outcome of the decision. This statutory codification emphasises that directors are supposed to make business judgements and that the legal test is for these judgements to be made rationally and on an informed basis.

OTHER LEGAL OBLIGATIONS

Company directors are also subject to a range of legal obligations, including those under various federal and state/territory tax and revenue laws, workers' compensation laws, consumer protection laws, consumer credit laws, equal opportunity laws, sexual harassment laws, environmental laws, Modern Slavery legislation, WHS laws and industrial agreements. Directors can be held personally liable under many of these laws and should seek legal advice if unsure of their obligations.

OTHER LEGAL OBLIGATIONS FOR DIRECTORS OF SUPERANNUATION TRUSTEES

Directors of superannuation trustees (as an RSE Licensee) owe additional obligations over and above the Corporations Act.

Unlike the Corporations Act, these duties are owed directly to members and beneficiaries of the superannuation fund. This is in addition to the duties owed by the Trustee itself (usually a corporate entity).

The trustee director duties include:

- a duty to act honestly in all matters concerning the entity;
- to exercise the same degree of care, skill and diligence as a prudent superannuation entity director would exercise;
- to exercise the director's powers as director of the corporate trustee in the best financial interests of the beneficiaries;
- where there is a conflict of interest, to give priority to the duties to and interests of the beneficiaries over the duties to and interests of other persons; and
- to exercise a reasonable degree of care and diligence for the purposes of ensuring that the corporate trustee carries out the covenants.²²

It is important to note that the obligation to act in the best financial interests of beneficiaries overrides any conflicting core directors duties in the Corporations Act.²³

The remainder of this section focuses on general Corporations Law duties. Directors of superannuation trustees should be mindful that further additional obligations apply in this context.

²² *Superannuation Industry (Supervision) Act 1993* (Cth) (SIS Act) s 52(2A))

²³ SIS Act s 52(3).

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

DIRECTORS' INDEMNITIES AND INSURANCE

Directors must understand the extent of their potential personal liabilities, and the extent to which they can be indemnified for these liabilities through indemnities granted by the company and the provision of directors' and officers' liability insurance (D&O insurance).

The Corporations Act precludes indemnification of officers (including directors) by a company against:

- liabilities owed to the company or a related body corporate
- liabilities owed to other parties that do not arise out of conduct in good faith
- certain liabilities for pecuniary penalties and compensation orders
- certain legal costs.²⁴

A company is prohibited from obtaining insurance to cover officers (including directors) against liabilities arising out of conduct involving:

- a wilful breach of duty in relation to the company
- a contravention of the duties of officers (and others) to not improperly use their position or information they obtain due to their position.²⁵

Given these limitations in company indemnities, public companies, in particular, nearly always take out D&O insurance on behalf of their directors. Various forms of D&O insurance are available, providing different levels of protection for the individual director. The director should ensure that the level of insurance cover is appropriate. The level of cover should be reviewed on an annual basis.

Details of any indemnification or insurance must be set out in the directors' report.²⁶

Directors should ask for a copy of the policy and any deed of indemnity and insurance the company has in place for the benefit of the directors. Directors should ensure that the level of cover is appropriate to their particular circumstances.

²⁴ Corporations Act 2001, Section 199A.

²⁵ Corporations Act 2001, Section 199B.

²⁶ Corporations Act 2001, Section 300(1) (g).

CONFLICT AND DISCLOSURE OF INTERESTS

Conflicts of Interest

A director should avoid being in a position where other interests or duties conflict with their duty to the company. Conflicts of interest can arise in several ways including:

- director contracts with the company (e.g. for the supply of services)
- related-party loans, guarantees and other securities
- profiting from a business opportunity that belongs to the company.

Sometimes a conflict is unavoidable. In such a case, the directors are obliged to disclose their conflict of interest or duty and take appropriate action to avoid any adverse consequences.

Directors should tread cautiously when considering an actual, potential or perceived conflict of interest. Any actual or potential conflicts of interest are best dealt with by way of full disclosure to the board.

Moreover, company stakeholders and the media can be highly critical of director conduct that can be perceived as self-serving. The reputations of both individual directors and their companies can suffer dramatically.

Material personal interests

The Corporations Act requires a director with a material personal interest in a matter relating to the affairs of a company to notify the other directors of that interest.²⁷ The constitution may also contain additional disclosure obligations. Whilst the Corporations Act does not define 'material personal interest', case law requires that materiality be considered in the context of the director (not the company) and must be personal to the director. That is, courts will look at the substance of the interest, its nature and capacity to influence the director's discharge of their fiduciary duties.²⁸

²⁷ Corporations Act 2001, Sections 191(1) and 191(2).

²⁸ See, for example, *Grand Enterprises Pty Ltd v Aurium Resources Ltd* (2009) 256 ALR 1 and *McGellin v Mount King Mining* (1998) 144 FLR 288.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The company's notification requirements are typically set out in the director's letter of appointment, and often certain disclosures are required for the office being accepted. The notification must detail the nature and extent of the interest and how the interest relates to the affairs of the company, and must be provided as soon as practicable after the director becomes aware of the relevant interest.²⁹ A director may give other directors standing notice about an interest.

Subject to certain exceptions, directors of a public company cannot vote on any matters in which they have a personal material interest, or be present while such matters are being considered at a meeting.³⁰ However, the other directors may pass a resolution which identifies the nature and extent of that director's interest and its relation to the affairs of the company, and permit the director to vote notwithstanding the interest.³¹ This approval must be recorded in the minutes of the meeting.

Depending on the extent of the conflict of interest, disclosure and abstaining from voting may not fully discharge a director's duty. There could be circumstances where a director needs to take further actions to protect the company's interests. For example, a director who has not yet made a formal notification in respect of a conflict could instruct the company secretary to withhold relevant information, such as board papers pertaining to the conflict.

In extreme cases, a director's resignation may be the only effective means of avoiding a serious conflict of interest.

RELATED PARTY TRANSACTIONS

Restrictions on related party transactions apply to a wide range of entities including public companies, or entities controlled by a public company, and there are significant procedural steps involved in managing such transactions, which are designed to protect shareholders' interests. For the purposes of the Corporations Act, a 'related party transaction' is any transaction through which a public

company or controlled entity provides a financial benefit to a 'related party' (which includes directors, their spouses, parents and children), and which by their nature raise a risk of a conflict of interest.³²

In general, a public company or its controlled entities must not undertake a transaction with a 'related party' unless it is approved by the company's members or the transaction otherwise falls within one of the relevant exemptions in the Corporations Act.³³ Where a company seeks and obtains the approval of its members to give a financial benefit to a related party, the benefit must be provided within 15 months of the approval being given.³⁴

Related party status endures for six months after the entity concerned ceases to be a related party.³⁵ Related party status also applies if the entity believes, or has reasonable grounds to believe, that it is likely to become a related party at any time in the future.³⁶ Further, an entity will be a related party if it acts in concert with a related party of a public company on the understanding that, if the company gives the entity a 'financial benefit', the related party will also receive a 'financial benefit'.³⁷

The term 'financial benefit' has a wide application, encompassing a multitude of potential transactions – including 'indirect' transactions through interposed entities, informal or oral agreements, agreements that have no binding force, and transactions that do not involve paying money.³⁸

Although failure to obtain member approval for conferring the financial benefit will not invalidate the contract or transaction, a director may be held to have committed an offence if they are involved in this failure and the involvement is dishonest.³⁹

²⁹ Corporations Act 2001, Section 191(3).

³⁰ Corporations Act 2001, Section 195.

³¹ Corporations Act 2001, Section 195(2).

³² Refer to Section 228 of the Corporations Act 2001 for definition of 'related party'.

³³ Sections 208 and 210-216 of the Corporations Act 2001.

³⁴ Corporations Act 2001, Section 208(2).

³⁵ Corporations Act 2001, Section 228(5).

³⁶ Corporations Act 2001, Section 228(6).

³⁷ Corporations Act 2001, Section 228(7).

³⁸ Corporations Act 2001, Section 229(2).

³⁹ Corporations Act 2001, Section 209(3).

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The ASIC Regulatory Guide 76 Related Party Transactions⁴⁰ provides useful guidance on the application of the Corporations Act and ASIC's expectations with regards to various aspects of related party transactions.

Accounting standards have a broader definition of 'related party' and require disclosure of related party transactions. Some of these related party disclosures are now required to be disclosed in the remuneration report for listed companies under the Corporations Regulations.⁴¹

INSOLVENT TRADING AND SAFE HARBOUR

Directors also have a positive duty to ensure that the company does not trade whilst it is insolvent.⁴² Directors who permit a company to incur a debt, where there are reasonable grounds for suspecting that the company is *already* insolvent or that incurring the debt will cause insolvency, may contravene section 588G of the Corporations Act. In certain circumstances, directors may be held personally liable for the debts incurred if the company trades whilst being insolvent. A company will be deemed to be insolvent if it is not able to pay its debts as and when they become due and payable.⁴³

However, if after suspecting insolvency, or that the company may become insolvent, a director starts developing or takes a course of action that is reasonably likely to lead to a better outcome for the company than the immediate appointment of an administrator or a liquidator,⁴⁴ the director will not be liable for debts incurred directly or indirectly in connection with the course of action,⁴⁵ provided certain conditions are met (as set out in further detail below).

It should be noted that directors wishing to rely on this exception will bear the evidentiary burden of establishing that they took the necessary action.⁴⁶

40 ASIC, 2011, Regulatory Guide 76, Related party transactions, <https://download.asic.gov.au/media/1239851/rg76-published-11-may-2011.pdf>

41 AASB 124 and Corporation Regulation 2M.3.03.

42 Corporations Act 2001, Section 588G.

43 Corporations Act 2001, Section 95A.

44 Corporations Act 2001, Section 588GA(1)(a).

45 Corporations Act 2001, Section 588GA(1)(b).

46 Corporations Act 2001, Section 588GA(3).

Some practical implications for directors

Developing and undertaking a course of action to achieve a better outcome is no mean feat. In examining a selected course of action, directors should have regard as to whether:

- appropriate steps are being taken to ensure a company is keeping appropriate financial records consistent with the size and nature of the company, and to prevent the officers or employees of the company from engaging in misconduct that could limit the entity's ability to pay its debts
- they are always keeping themselves properly informed of the company's financial position
- they are developing or implementing a plan to restructure the company to improve its financial position
- an appropriate level and extent of advice is being sought from an appropriately qualified professional and whether sufficient information has been provided to the professional to facilitate the giving of sound advice.

It should be noted that regard may be had to the above factors in formal proceedings as part of the assessment of whether a course of action was 'reasonably likely' to result in a better outcome for the company.⁴⁷

Ultimately recognising the early signs of distress and taking early action remains the best way for directors to improve their chances of achieving a better outcome for the company and its stakeholders.

Where safe harbour is not available

If a company is not able to take advantage of the safe exception, there is a defence that the director had reasonable grounds to expect, and did expect, that the company was solvent.⁴⁸ This defence usually requires a careful assessment of the company's circumstances to determine whether they provide a director with the requisite 'reasonable grounds' to expect solvency.

47 Corporations Act 2001, Section 588GA(2).

48 Corporations Act 2001, Section 588H(2).

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Insolvent trading 'red flags'

Directors should constantly be on the lookout for signals that may suggest their company's financial reporting is misleading or disguising a serious deterioration in its financial stability. An understanding of the company's financial position at the time of sign-off of the yearly financial reports is insufficient. Insolvent trading 'red flags' that raise concerns for directors include:

- irregular financial reporting
- lack of management focus on key ratios
- insufficient and immature liquidity analysis of the company's debt profile
- lack of budgets or in-depth analysis of failure to meet budgets.

Directors' responsibilities during insolvency

Insolvency, or the threat of insolvency, requires directors to act in the interest of creditors. It is a situation in which directors must subordinate the interests of shareholders to those of the company's creditors. In this context, directors should note that the company must not pay a dividend unless:

- the company's assets exceed its liabilities immediately before the dividend is declared and the excess is sufficient for the payment of the dividend
- the payment of the dividend is fair and reasonable to the company's shareholders as a whole
- the payment of the dividend does not materially prejudice the company's ability to pay its creditors.⁴⁹

The issue of insolvent trading is accentuated as corporate structures become more complex and parent companies become responsible for the affairs of numerous 'controlled entities'. From a Corporations Act perspective, the concept of a controlled entity is not confined to a wholly-owned subsidiary. A company can be said to control another if it has the capacity to dominate the decision-making of the other entity, or to impose its interests on the other entity.

⁴⁹ Corporations Act 2001, Section 254T(1).

Boards should seek professional advice if there is any doubt as to whether an entity is a 'controlled entity'.⁵⁰

ASIC Regulatory Guide 217 'Duty to prevent insolvent trading: Guide for directors' provides useful guidance around the key principles that directors need to take into account in order to comply with their duty to prevent insolvent trading.⁵¹

CONTINUOUS DISCLOSURE

The Corporations Act and the ASX Listing Rules impose duties on the officers and employees of listed and unlisted disclosing entities to make immediate disclosures to markets about certain materially price sensitive information.⁵²

The board has general oversight of an entity's disclosure obligations. The board will often delegate its powers to a disclosure committee or other senior executives within the organisation for the day-to-day management of disclosure issues. However, the board cannot delegate its responsibility for disclosure in a number of circumstances, for example, financial reporting. The Governance Institute of Australia (GIA) suggest that it may be useful to include a continuous disclosure confirmation as the final item of business on listed entity board agendas and to appoint a disclosure officer who can report to the board on continuous disclosure. Consideration of disclosure issues should form part of the board and executive considerations, and should be part of team discussions and culture within an organisation.⁵³

Under Listing Rule 3.1, 'once an entity is or becomes aware of any information concerning it that a reasonable person would expect to have a material effect on the price or value of the entity's securities the entity must immediately tell the ASX that information'.⁵⁴ There are, however, limited exceptions to this obligation prescribed under the ASX Listing Rules.⁵⁵

⁵⁰ Directors should be aware that the Corporations Act 2001 definition of 'control' of another entity differs from the definition of 'control' as contained in AASB 10 Consolidated Financial Statements.

⁵¹ ASIC, 2010, Regulatory Guide 217, Duty to prevent insolvent trading: Guide for directors, <https://download.asic.gov.au/media/1241384/rg217-29july2010.pdf>

⁵² Sections 674–675 of the Corporations Act 2001 and ASX Listing Rule 3.1.

⁵³ Refer to GIAs 'Continuous disclosure: listed and other disclosing entities' guidelines.

⁵⁴ Refer to ASX, Chapter 3, Continuous disclosure, <https://www.asx.com.au/documents/rules/Chapter03.pdf>

⁵⁵ ASX Listing Rule 3.1A.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The continuous disclosure framework is designed to ensure that the market is fully informed at all times and that all investors have access to material information. Sustainable investment indices rely either wholly or in part on the public disclosure of relevant information by listed entities. It is widely recognised that there are significant financial and reputational benefits to companies whose practices are recognised through favourable ratings from such indices. Those ratings can be significantly enhanced by good governance practices in connection with continuous and periodic disclosure or, conversely, damaged by poor practices.⁵⁶

With the introduction of the *Treasury Laws Amendment (2021 Measures No 1) Act 2021*, the continuous disclosure obligations were modified such that now,⁵⁷ companies and officers will only incur liability in breach of their continuous disclosure obligations if they had acted with the requisite 'knowledge, recklessness or negligence'.⁵⁸ The implications of introducing such fault elements allows 'companies to more confidently make forecasts of future earnings or provide guidance updates without facing the undue risk of class actions'.⁵⁹ These changes together with others announced by the ASX in March 2025 (Compliance Update No. 02/25)⁶⁰ have been further discussed in [Chapter 7](#).

Share price and media monitoring

The ASX strongly encourages an entity that is relying on the exemptions to disclosure about a market sensitive transaction it is negotiating, or that otherwise chooses not to request a trading halt or voluntary suspension in advance of its market sensitive announcement, to monitor 'blogs, chat-sites and other social media that regularly post comments about the entity' for any signs the information has been leaked.⁶¹

⁵⁶ Refer to GIA's 'Continuous disclosure: listed and other disclosing entities' guidelines.

⁵⁷ Corporations Act 2001, Sections 674 and 675.

⁵⁸ Corporations Act 2001, Sections 674A and 675A.

⁵⁹ The Hon Josh Frydenberg MP, Media Release <https://joshfrydenberg.com.au/latest-news/permanent-changes-to-australias-continuous-disclosure-laws/>

⁶⁰ ASX, <https://www.asx.com.au/content/dam/asx/documents/listings/compliance-updates/2025/listed-at-asx-compliance-update-4-march-2025.pdf>

⁶¹ Refer to ASX, Chapter 3, Continuous disclosure, <https://www.asx.com.au/documents/rules/Chapter03.pdf>

Monitoring the share price of an entity is necessary to ensure that any suspected leaks of confidential information can be quickly identified and dealt with. Monitoring media, including social media, is also useful in identifying whether the market may be operating on the basis of false information. Reporting services are available to assist with collating media reports.

INSIDER TRADING

Under the Corporations Act it is an offence if a person with 'inside information' applies for, acquires or disposes of securities, or enters into an agreement to do any of those things. A person with inside information is also prohibited from procuring another party to do any of those things.

The purpose of the insider trading regime is to ensure that the securities market operates freely and fairly with all participants having equal access to relevant information so that no party has an unfair advantage over another. Refer to the 'share trading by directors' section of this chapter for further information.

By virtue of their roles, directors and officers of companies will be privy to inside information and should, therefore, take particular care to ensure they observe the prohibition against insider trading in the Corporations Act. Insider trading involves the misuse of price-sensitive company information that is not generally available.

Importantly, an 'insider' can be a natural person or a corporation, and need not be directly associated with the company. The Corporations Act prohibits any person in possession of inside information from:

- dealing – applying for, acquiring or disposing of the relevant financial products or entering into an agreement to do any of these things (trade)
- procuring – enabling another person to trade in those financial products
- tipping – communicating the information, or causing the information to be communicated, to another person who is likely to trade in those financial products, or procure someone else to so trade.⁶²

⁶² Corporations Act 2001, Section 1043A.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

For the purposes of the insider trading provisions of the Corporations Act, the definition of 'financial products' is contained in section 1042A of the Corporations Act and includes, for example, shares, debentures, options and any other product that is able to be traded on a financial market.

Under the continuous disclosure provisions of the Corporations Act and ASX Listing Rules, listed companies will, in general, have disclosed all price-sensitive information to the market as it becomes available. Accordingly, in practice, the insider trading restrictions will generally apply to price-sensitive information that has been withheld from disclosure pursuant to one of the exceptions (e.g. an incomplete proposal for a takeover).

Generally, around the time of the results announcement/annual general meeting is the most 'pure' or 'clean' time when a company is least likely to have insider information.

Further, a company should have a securities trading policy in place to prevent the misuse of insider information.

In relation to unlisted companies, directors should take particular care in relation to a capital or debt raising, or share transfers in relation to the company, where there may not be equal knowledge of the company's activities by parties to the proposed raising or share transfer.

Insider trading is a serious offence attracting substantial fines and potential imprisonment. Civil liability may also attach to the offence.

RECORD KEEPING

The Corporations Act also requires that directors are personally responsible for preparing and maintaining key documents and reports. Directors are required to keep, either in hard or soft copy:

- up-to-date financial records that accurately reflect the company's financial position, including transaction level details (i.e. general ledger, cash balances, wage and salary details, debtor and creditor listings, property/asset register, tax returns and details of investments)

- registers of members (shareholders), including option holders (if applicable)
- minutes of general meetings
- minutes of meetings of directors
- registers of charges created by the company over company property.⁶³

Financial records must be kept by all entities covered by the Corporations Act, however a 'small proprietary company' or a small company limited by guarantee (as defined in the Corporations Act), is not generally required to prepare and submit an annual report to ASIC. Larger companies (including not-for-profits) are required to lodge audited financial statements to ASIC each year, with exceptions for some public companies limited by guarantee.⁶⁴ Further, charities who are registered with the Australian Charities and Not-for-profits Commission (ACNC) are required to lodge either an annual information statement or a financial report (depending on their size) with the ACNC as opposed to ASIC.⁶⁵

SHARE TRADING BY DIRECTORS

Subject to the general prohibition against insider trading, the ASX Listing Rules, and the restrictions applying to directors under the share trading policy of a listed company, directors can, in certain circumstances, buy and sell shares and other securities in their companies.

ASX listed companies are required to have a share trading policy restricting dealing in the company's securities by its directors and other key management personnel.⁶⁶

⁶³ ASIC, Information Sheet 79, Your company and the law, <https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/your-company-and-the-law/>

⁶⁴ For more details on record keeping obligations, see ASIC Information Sheet 131 <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/preparers-of-financial-reports/companies-limited-by-guarantee/obligations-of-companies-limited-by-guarantee/> and ASIC Information Sheet 76 <https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/what-books-and-records-should-my-company-keep/>

⁶⁵ Section 111L of the Corporations Act 2001 and Australian Charities and Not-For-Profits Commission Act 2012 (Cth), division 60.

⁶⁶ See ASX Listing Rule 12.9 and ASX Listing Rules Guidance Note 27 – 'Trading Policies' and Recommendation 1.3 of ASX Corporate Governance Principles and Recommendations (4th edition).

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Under such policies, the directors and other key management personnel are restricted from trading in the company's securities during specified 'prohibited periods' (often referred to as 'black-out' or 'closed' periods – typically for a period before the release of financial results), and/or only permitted to trade during certain defined 'trading windows' (e.g. after the public release of financial results).

The Corporations Act requires directors of listed companies to notify the ASX of any interests they have in the securities of their listed company (or a related body corporate), and of any contracts to which they are a party, or from which they are entitled to a benefit.⁶⁷ The ASX Listing Rules also contain similar notification requirements, although the notification obligation rests with the listed entity, rather than the director.⁶⁸

RESIGNATION

The *Treasury Laws Amendment (Combating Illegal Phoenixing) Act 2020*, resulted in the *Corporations Act* being amended such that directors have additional obligations regarding their resignation. Specifically, a director's resignation will only be effective on the date that the person ceases to be a director if notice of this resignation is lodged with ASIC within 28 days of its occurrence.⁶⁹

If lodged later than 28 days but within 56 days, an application can be made to ASIC providing reasons, with ASIC having the liberty to accept the application and fix the resignation date as the claimed resignation date.⁷⁰ Should this notice not be received within 28 days and an application is not made to ASIC within 56 days or less, the date of the director's resignation will only take effect the date the notice is received by ASIC.⁷¹ Ultimately, tenure of a director will be artificially extended until such time notice of their resignation is lodged.

In instances where the resignation of the director or the passing of a resolution to remove a director will leave the company without any directors, the resignation will be deemed void, though note that exceptions exist for companies being wound up.

ENFORCEMENT, PENALTIES AND REMEDIES

Directors who breach their legal responsibilities face a range of criminal and civil penalties, and can also expect to suffer damage to their reputations and their professional or commercial careers. Moreover, it can also affect the company's reputation.

As summarised by Rod Sims, former ACCC Chair, 'as a company director you have a responsibility to ensure that your company is meeting its legal obligations. Beyond the good corporate citizen aspects of compliance, now more than ever the costs of non-compliance are significant. The impact of regulatory action, with increasing penalties and costly litigation, is one thing; lost reputation, reduced customer trust, distracted management and remedial actions also take their toll on companies'.⁷²

⁶⁷ Corporations Act 2001, Section 205G. See also ASIC Regulatory Guide 193 <https://download.asic.gov.au/media/1241069/rg193.pdf>

⁶⁸ ASX Listing Rules 3.19A and 3.19B. See also ASX Guidance Note 22 – 'Director disclosure of Interests and Transactions in Securities – Obligations of Listed Entities'.

⁶⁹ Corporations Act 2001, Section 203AA.

⁷⁰ Refer to ASIC, Resigning or removing a company director, <https://asic.gov.au/for-business/small-business/starting-a-company/small-business-company-directors/resigning-or-removing-a-company-director/>

⁷¹ Corporations Act 2001, Section 203AA.

⁷² Refer to Section 3.3.1 of the 'AICD's Essential Director Update:18' <https://aicd.companydirectors.com.au/membership/membership-update/essential-director-update-18-highlights>

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Criminal penalties

In certain circumstances, directors can be charged with criminal offences. Criminal penalties can be imposed for a number of actions including:

- if a director is reckless or dishonest, and fails to act in good faith, in the best interests of the company or for a proper purpose
- breach of other statutory duties, such as the duty not to make improper use of a director's position or of information received as a director
- contravention of the prohibition against insider trading.

Directors found guilty of these criminal breaches can be fined and/or imprisoned.

Industrial manslaughter laws

Following a Senate Inquiry, the Education and Employment References Committee published its report in October 2018 titled 'They never came home – the framework surrounding the prevention, investigation and prosecution of industrial deaths in Australia'. One of the key recommendations was 'the formal harmonisation of WHS laws process' in each state and territory.⁷³

Industrial manslaughter was first introduced in Australia when it was passed by the Australian Capital Territory's Legislative Assembly on 27 November 2003 under the *Crimes (Industrial Manslaughter) Amendment Act 2002* (ACT), which took effect on 1 March 2004.

In December 2018, Maria Carla Jackson, 72, was the first individual in Victoria to be sentenced to prison under the breach of duty provisions of occupational health and safety legislation. Ms Jackson was convicted and sentenced to six months jail under the Victorian Occupational Health and Safety Act 2004, after the death of a man at her scrap metal yard in Foster, Victoria.

⁷³ Refer to Recommendation 5 of the report, available at https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024170/toc_pdf/Theynevercamehome%e2%80%94theframeworksurroundingtheprevention%20investigationandprosecutionofindustrialdeathsinAustralia.pdf;fileType=application%2Fpdf

Robbie Blake was killed when he fell three metres from a raised forklift (being operated by Ms Jackson, who did not hold a forklift licence) and was hit by a falling bin in February 2017. Ms Jackson pleaded guilty to breaching the Occupational Health and Safety Act by failing to comply with her duty as a self-employed person not to expose other people to risk.⁷⁴

Accordingly, it is important that directors understand their responsibilities regarding workplace health and safety and are receiving the necessary information to be able to understand whether the control environment is aligned to their risk appetite. Chapter 21 *Health, Safety and Wellbeing* discusses how industrial manslaughter laws are being approached in each state.

Civil penalties

Civil penalties can apply to a range of breaches of statutory duty, including:

- the duty to exercise reasonable care and diligence
- the duty to act in good faith in the best interests of the company and for a proper purpose
- related party rules
- market manipulation
- the duty to prevent insolvent trading.

Directors who have benefited from a breach of duty may also be ordered to account for any profits received. Penalties can include fines, a disqualification order or a compensation order. In civil proceedings, the burden of proof is on the balance of probabilities, rather than beyond the reasonable doubt demanded in criminal proceedings.⁷⁵

⁷⁴ Hook. M, 2019, <https://www.abc.net.au/news/2019-01-25/victorian-junkyard-woman-sentenced-to-jail-over-death/10746110> and WorkSafe Victoria, Prosecution Result Summaries and Enforceable Undertakings, <https://www.worksafe.vic.gov.au/prosecution-result-summaries-enforceable-undertakings>

⁷⁵ See ASX Listing Rules Guidance Note 27 and Recommendation 1.3 of ASX Corporate Governance Principles and Recommendations (4th edition)

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

CASE STUDY



Case study: Storm Financial

In March 2020, the Federal Court rejected Cassimatis' appeal and upheld their 2018 penalties judgement in the Storm Financial matter. It brought to an end the long-running ASIC litigation arising out of the collapse of the Queensland financial planning business a decade ago.

The court held that Mr and Mrs Cassimatis, both executive directors of Storm Financial, had contravened their duty of care and diligence under section 180(1) of the *Corporations Act 2001*. Their conduct facilitated Storm to provide the 'Storm model' of financial advice to a group of financially vulnerable investors. In doing so, they caused or permitted Storm to contravene the financial services laws and exposed it to the risk of losing its AFS licence. Mr and Mrs Cassimatis were each ordered to pay civil penalties of \$70,000 and disqualified from managing corporations for seven years.

Cassimatis v Australian Securities and Investments Commission (ASIC) [2020] FCAFC 52



Case study: the collapse of HIH Insurance

The demise of HIH Insurance Limited (HIH) is considered to be the largest corporate collapse in Australia's history. HIH was Australia's second largest general insurer. In 2001, HIH and a number of its subsidiaries were placed into liquidation with losses of \$800 million. The main reasons cited for the HIH collapse were poor management and greed, characterised by a lack of accountability for performance, lack of integrity in internal processes, and lack of attention to detail and skills. [FN55]

'The governance of a public company should be about stewardship. Those in control have a duty to act in the best interests of the company. They must use the company's resources productively. They must understand that those resources are not personal property.' – **Report of the HIH Royal Commission (Justice Owen), April 2003**

ASIC v Adler & Ors (2002) NSWSC 171

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US



Case study: James Hardie Industries Limited

In May 2012, the High Court found that seven former non-executive directors of James Hardie Industries Limited (James Hardie) had breached their duties as directors when they approved the release of a misleading ASX announcement regarding the foundation which was established to cover the asbestos claims made against the James Hardie group. The ASX announcement stated that the foundation was 'fully funded' for the purposes of meeting all future compensation claims, when in actual fact there was a funding shortfall of more than \$1.5 billion.

The High Court also separately determined that the former James Hardie company secretary and general counsel, Mr Shafron, had contravened section 180(1) of the Corporations Act (the duty of care and diligence) by failing to properly advise the board and CEO in relation to the establishment of the asbestos foundation.

The High Court remitted the case to the NSW Court of Appeal to hear the directors' appeals on penalties and relief from contravention. In November 2012, the NSW Court of Appeal imposed fines on the non-executive directors and banned each of them from being involved in the management of a corporation for varying periods of time (which was a reduction of the original penalties and disqualification periods that had been imposed by the NSW Supreme Court). In respect of Mr Shafron, the court reinstated the fine and disqualification period imposed by the trial judge (namely a \$75,000 fine and disqualification period of seven years).

ASIC v Hellicar [2012] HCA 17

ASIC Media Releases: 12-275MR (Decision in James Hardie penalty proceedings) and 12-85MR (Decision in ASIC's appeals in James Hardie Matter)

Remedies

A cause of action may also arise under general law against directors for breach of:

- the duty of care and diligence arising from common law negligence
- contractual obligations
- the equitable duty to exercise reasonable care and skill.

In addition, if a director breaches the fiduciary duties owed to the company and it suffers a consequential loss, the company may pursue compensation by way of equitable remedy. This is similar to the common law remedy of damages.



FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- ASIC Regulatory Guide 76 – Related party transactions, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-76-related-party-transactions/>
- ASIC Regulatory Guide 217 – Duty to prevent insolvent trading: Guide for directors, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-217-duty-to-prevent-insolvent-trading-guide-for-directors/>
- Australian Institute of Company Directors, <http://aicd.companydirectors.com.au>
- Lipton, P., Hertzberg, A. and Welsh M., Understanding Company Law, 16th edition, Thomson Reuters Australia Limited, 2012.

For further information
please contact:



Caron Sugars
Lead Partner,
Board Advisory Services
KPMG Australia
ccobargsugars@kpmg.com.au

For Financial Services related
information, please contact:



Dr Lisa Butler Beatty
Partner, Superannuation
Advisory Lead
KPMG Australia
lisabbeatty@kpmg.com.au

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

2. Governance Roles

There are many instruments, roles and responsibilities required for a board to deliver its governance function effectively. Key factors such as independence, board composition and skills play a critical role in board performance.

In this chapter

- Governance scope
- Board charter
- Annual board agenda
- Retained authorities
- Delegated authorities
- Accountabilities framework
- Types of directors
- Chair's role
- Deputy chair or senior independent director
- Company secretary's role
- Induction and professional development

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Is the composition of the board appropriately diverse for it to perform effectively?
2. Is the board sufficiently independent of management to enable it to make tough decisions?
3. Is a regular assessment of each director's independence made by the board?
4. Does the board periodically review the board and chair's performance, and if so, is the review done by an external body?
5. Does the board tailor its charter to the organisation's circumstances and is the charter periodically reviewed?
6. Is there an annual agenda, approved by the board that is linked to the board's key responsibilities, as detailed in the board charter?
7. Are matters that must be referred to the board for approval clearly articulated to management?
8. Does the board clearly set out the roles and authority of the CEO and directors in writing?
9. Are delegations to management, including the delegations policy, set out in a single document?
10. Is the board monitoring that directors allocate sufficient time to discharge their responsibilities?

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The board spends too much time on operational matters with limited time for strategic discussions.
- Policies and procedures are not updated regularly.
- The board is heavily weighted towards a certain skillset, background, or gender.
- Some directors have family ties or cross-directorships that have not been discussed or are overlooked.
- Assessments of director independence are informal and infrequent.
- The board's charter is outdated with the last date of review unknown.
- A statement of 'matters reserved to the board' does not exist, or is not explicit and clear.
- There are no board approved instruments, such as a code of conduct and delegations of authority.
- Assessments of the board's performance are only done internally (or not at all) and are routinely positive with little to no action taken to address any opportunities for improvement identified.
- The director induction process is procedure-based only.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

GOVERNANCE SCOPE

At its very centre, the role of the board is governance of the organisation. Governance is a unique concept and very different to management, which is the role and function of the executive team. Governance requires a balance between a 'hands-off' approach to implementation, and a greater focus on **oversight, insight** and **foresight** in the context of stewardship, direction-setting and monitoring performance of the management team against the approved strategic objectives.

The board's governance scope refers to the key roles and responsibilities of the board and includes the following key functions:

- developing, along with senior management, the company's vision, purpose, core values, strategic direction and objectives
- evaluating and challenging management's recommendations on important strategic and operational matters
- holding management to account for its performance and decisions
- scrutinising key financial and non-financial risks to which the enterprise is exposed and ensuring the implementation of an effective risk management, compliance and internal control framework
- ensuring the adequacy of internal regulatory and policy compliance systems
- setting and demonstrating the corporate culture of the organisation
- adopting appropriate ethical standards, code of conduct and appropriate behaviours, and ensuring that these are adhered to at all times
- communicating and reporting to shareholders and other stakeholders in a transparent and insightful manner
- overseeing management succession plans
- evaluating the board's own practice and performance and the contribution of individual directors.

The board's governance scope should be clearly documented in the board charter.

BOARD CHARTER

The ASX Principles state in Recommendation 1.1 that a listed entity should have and disclose a board charter setting out:

- the respective roles and responsibilities of its board and management and
- those matters expressly reserved to the board and those delegated to management.

The purpose of a board charter is to document the board's terms of reference, and to articulate the board's approach to important governance practices. The charter should contain a statement clarifying the division of responsibilities between the board and management. Many boards define the roles, powers and responsibilities that it specifically reserves for itself, and those which it delegates to management.

All entities, whether private, public, listed, non-listed, not-for-profit or government, should have a document that clearly outlines the board's purpose, functions and key operating mechanisms. The document could be called a Charter, By-laws (in the case of government entities) or Terms of Reference. For the purposes of this discussion, we will use the term 'Charter'.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

While the content of the board Charter will vary, the board Charter of an ASX listed company (which can be used as better practice guidance for non-listed entities) will typically cover the following matters:

- overview of board roles, functions and responsibilities
- board structure and composition
- the chair's role
- the role of the company secretary
- the board's policy for assessing independence
- retained authorities
- board delegations
- board meeting procedures
- oversight of strategy, financial and risk management, and remuneration frameworks.

The board should periodically review its Charter to ensure it remains relevant to the circumstances of the company. The Charter should be available to directors, management, staff, auditors and shareholders. The ASX Principles recommend that the roles and responsibilities be set out in a Charter or some other document published on the company's website.¹

See *Appendix 1 Board Charter for an example.*

ANNUAL BOARD AGENDA

Boards commonly formulate an annual board agenda as an effective planning tool. The chair should refer to the annual agenda before approving the agendas for individual board meetings.

An effective annual agenda will:

- provide coverage of all the board's key activities
- provide adequate time for discussion
- ensure all the obligations included in the charter will be addressed
- provide opportunities for the continuous development of directors.

The annual agenda can also be used as an evaluation tool to assess whether the board has achieved the activities planned in the agenda.

See *Appendix 2 Annual Agenda for an example.*

RETAINED AUTHORITIES

The ASX Principles encourage all companies (both listed and non-listed) to disclose the respective roles of its board and management and adopt a formal statement of matters reserved for the board's decision or a formal board charter that specifies its functions and responsibilities.² The ASX Corporate Governance Council has compiled a list of responsibilities³ that boards normally reserve for themselves.

Some of these responsibilities include:

- demonstrating leadership, defining the entity's purpose and setting its strategic objectives
- appointing the chair and appointing and replacing the CEO
- approving the appointment and replacement of other senior executives
- overseeing the integrity of the entity's accounting and corporate reporting systems
- ensuring that the entity has in place an appropriate risk management framework (for both financial and non-financial risk)
- ensuring that the entity's remuneration framework is aligned with the entity's purpose, values, strategic objectives and risk appetite
- monitoring the effectiveness of the company's governance practices.

Some boards adopt a formal delegation of authority policy, delineating respective board and management authorities, while setting financial limits on decisions that can be made without specific board approval. Ensuring that the CEO and the board itself understand their respective roles and responsibilities is a priority of every board.

¹ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 6.1.

² *ibid.*, Recommendation 1.1.

³ *ibid.*, see commentary to Recommendation 1.1.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

DELEGATED AUTHORITIES

Given the complexity and size of the typical large business enterprise, it is not possible, nor is it desirable, for a board to exercise all of its possible powers and functions directly. The Corporations Act provides that, unless a company's constitution provides otherwise, directors may delegate any of their powers to a board committee, a director, an employee of the company, or any other person.⁴

Directors are entitled to rely on others, where they believe, on reasonable grounds at all times the delegate would exercise the power in conformity with the duties imposed on directors of the company under the Corporations Act and the company's constitution,⁵ and the director believed on reasonable grounds, in good faith and after making proper enquiries that the delegate was reliable and competent in relation to the power delegated.⁶ If these conditions are not met, the directors will be responsible for the exercise of power by the delegate as if the directors themselves had exercised the power.⁷

This provision implies that boards must take responsibility not only for the appointment of a reliable and competent CEO, but must also make a judgement about the competence of the entire senior management team, as well as being satisfied that the company has established proper processes for the hiring of competent employees.

In delegating their powers to committees or management, boards must:

- ensure the delegation is consistent with and in accordance with the entity's risk appetite
- demonstrate and maintain rigorous oversight over the exercise of those powers
- ensure that management and committee reporting back to the board strikes the right balance between summary and detailed information
- ensure seamless communication between board committees.

It is important that directors review materials and financial reports presented by management and auditors with a critical eye, and not accept or approve materials without question, to ensure that reasonable grounds exist to rely on the work of management (as was famously highlighted in the James Hardie and Centro cases).⁸ Case law makes it clear that directors cannot substitute reliance upon the advice of management for their own attention and examination of an important matter that falls within the board's responsibilities (such as, for example, reporting obligations).⁹

The delegations policy, which is approved by the board, should specify the limits of authority to take action and/or make financial and non-financial decisions for all individuals, including the delegations from the CEO to senior management and from senior management to staff. This will assist the board in fulfilling its duty of care and be a useful reference to all company personnel as to who has responsibility for decision-making.

⁴ Corporations Act 2001, 198D.
⁵ Corporations Act 2001, 190 (2)(a)
⁶ Corporations Act 2001, 190 (2)(b).
⁷ Corporations Act 2001, 190 (1).

⁸ ASIC Information Sheet 183

⁹ ASIC v Healey & Ors [2011] FCA 717 at 175.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ACCOUNTABILITIES FRAMEWORK

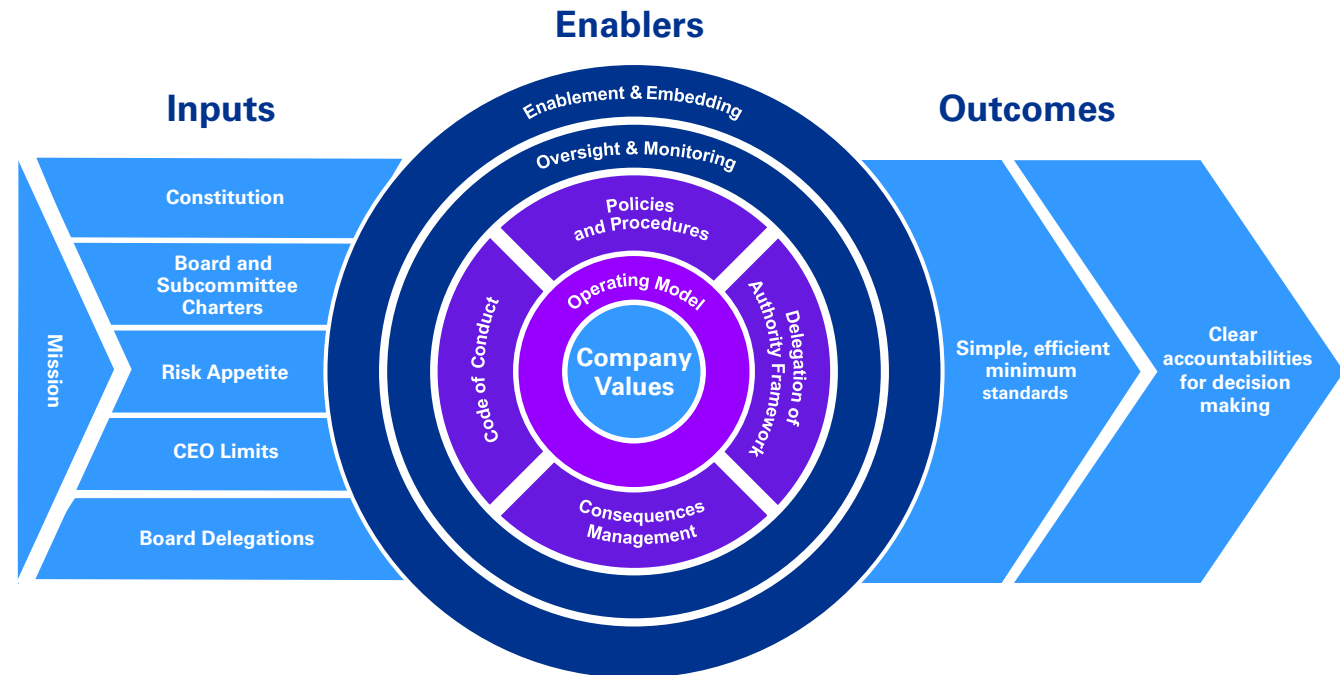
The KPMG accountabilities framework outlines below the inputs and enablers to deliver simple, efficient minimum standards and clear accountabilities for decision-making across the organisation.

To achieve an effective accountabilities framework requires the board to endorse these instruments, oversee their implementation and regularly consider their compliance and currency.

TYPES OF DIRECTORS

There are two principal types of directors: executive directors and non-executive directors. However, the Corporations Act also defines a range of other types of directors, that share the same overall fiduciary responsibilities, but with some slight differences. It is important to understand what type of director you are and how this impacts on your ability to effectively and lawfully fulfil the requirements of the role.

KPMG Accountabilities Framework



FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Non-executive directors

A non-executive director is a director who is not involved in the day-to-day management of the company and does not hold an executive position. They primarily attend board meetings and contribute to strategic oversight, governance, and risk management, rather than operational decisions.

Being independent of the management of the organisation, non-executive directors play a vital role. Although written in 2003, the Higgs Report,¹⁰ looking at the role and effectiveness of non-executive directors, is still relevant as it pertains to the main responsibilities of a non-executive director, being to:

- constructively challenge and contribute to the development of strategy
- scrutinise the performance of management in meeting agreed goals and objectives, and monitor the reporting of performance
- satisfy themselves that financial information is accurate and that risk management systems are robust and defensible
- appoint, evaluate and remove senior management personnel in line with succession plans
- determine appropriate levels of remuneration for executive directors.

This report also suggests that, in order to discharge their responsibilities, effective non-executive directors should possess key personal attributes:

- integrity and high ethical standards
- sound judgement
- ability and willingness to challenge and probe
- strong interpersonal skills.¹¹

An important characteristic of a non-executive director is the willingness to confront management and raise difficult issues. Non-executive directors must have '*sufficient strength of character to seek and obtain full and satisfactory answers within the collegiate environment of the board*'.¹²

¹⁰ Higgs, D., Review of the Role and Effectiveness of Non-Executive Directors, Department of Trade and Industry (UK) Jan 2003, P80 at para A1.4, <http://www.ecgi.org/codes/documents/higgsreport.pdf>

¹¹ *ibid.* p29 at para 6.12

¹² *ibid.* p 29 at para 6.15.

Independent directors

Independent directors play an important role in the separation of power between the management of the company, including executive directors, and can offer new perspectives and challenge old paradigms.

The ASX Principles recommend that a majority of the board should be independent directors.¹³ An independent director can be defined as 'a director who is free of any interest, position, or relationship that might influence, or reasonably be perceived to influence, in a material respect their capacity to bring an independent judgement to bear on issues before the board and to act in the best interests of the entity as a whole rather than those of an individual security holder or other party'.¹⁴

The ASX Principles go on to provide examples of interests, positions, affiliations and relationships that might raise issues about the independence of a director.¹⁵ These include if the director:

- is, or has been, employed in an executive capacity by the entity or any of its child entities and there has not been a period of at least three years between ceasing such employment and serving on the board
- receives performance-based remuneration (including options or performance rights) from, or participates in an employee incentive scheme of, the entity
- is, or has been within the last three years, in a material business relationship (e.g. as a supplier, professional adviser, consultant or customer) with the entity or any of its child entities, or is an officer of, or otherwise associated with, someone with such a relationship
- is, represents, or is or has been within the last three years an officer or employee of, or professional adviser to, a substantial security holder
- has close personal ties with any person who falls within any of the categories described above
- has been a director of the entity for such a period that their independence from management and substantial holders may have been compromised.

¹³ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 2.4

¹⁴ *ibid.*, Glossary definition

¹⁵ *ibid.*, Box 2.3

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

In each case, the materiality of the interest, position or relationship needs to be assessed by the board to determine whether it might interfere, or might reasonably be seen to interfere, with the director's capacity to bring an independent judgement to bear on issues before the board, and to act in the best interests of the entity as a whole, rather than in the interests of an individual security holder or other party.

The consultation draft for a proposed fifth edition of the Corporate Governance Principles¹⁶ reflected that in the next iteration direction may be provided as to what constitutes a substantial holder, this being denoted as 10%.

Directors considered by the board to be independent should be identified as such in the corporate governance statement of the annual report. The board should state its reasons if it considers a director to be independent and the corporate governance statement should disclose the existence of any relationships that might suggest otherwise. In this context, it is important for the board to consider materiality thresholds from the perspective of the company and the director, and to disclose these.

For some entities, having a majority of board members as independent directors may not be possible or appropriate. The size of the board, the nature of the business and the skills required, may limit the number of independent appointments. In this situation, it is important to ensure that the organisation has at least one independent director to provide challenge and perspective that only someone from outside the organisation can bring.

Executive directors

Executive directors are paid employees of the company. They are often members of the company's senior management team. The CEO may also be an executive director and in some cases other senior executives may also be appointed to the board.

¹⁶ ASX, Consultation Draft for a proposed fifth edition of the Principles and Recommendations, <https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/corporate-governance-principles-and-recommendations-consultation-draft.pdf>

In rare instances, a CEO may also be the chair of the board. Whilst there is no empirical evidence to suggest which model is better, combining these roles can see the lines between the board and management being blurred, requiring the individual to have a strong understanding of where and when they take on the relevant role.

Whilst in certain countries, like Germany, the practice of having a CEO appointed as chair is not allowed (for companies with a two-tier board system), this has historically been more common in the United States. It is notable, however, that this practice is reducing and the Wall Street Journal reported that as at April 2024 approximately 60% of S&P 500 companies have separate CEO and Chair roles according to S&P 500 proxy statements.¹⁷

In Australia, where the CEO is appointed chair, an explanation of why this is considered appropriate must be provided in the annual corporate governance statement. Recommendation 2.5 of the ASX Principles states that the chair of the board of a listed entity should not be the same person as the CEO of that entity.

The argument in favour of executive directors is that they add value to a board's decision-making process through their technical expertise and knowledge of the business and its industry.

The presence of executives on the board can be beneficial to the extent that they can inform non-executive directors by providing their relevant expertise and current working knowledge. Executives might also offer a valuable second opinion to the statements and recommendations of the CEO. A risk exists that their loyalty to the CEO could conflict with their statutory duty as directors to act in the best interests of the company.

Nominee directors

A nominee director is a director appointed by a shareholder, creditor or interest group. Nominee directors have the same overriding duty as other directors. However, they are often thought to have an ongoing allegiance to the nominator responsible for their appointment.

¹⁷ PR Newswire, 'Spencer Stuart U.S. Board Index Finds CEO Experience and Financial Expertise Remain Top S&P 500 Boardroom Recruiting Priority', 26 September 2024

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Whilst a nominee cannot favour the nominator's interests over that of the company, they can have regard to the interests of the nominator, provided that the nominee director ultimately acts for a proper purpose and in the best interests of the company. Where the interests of the nominator and the company diverge, the nominee should not participate in the decision.

A nominee director must not divulge to the nominator information obtained from the company in the nominee's capacity as a director if there is a conflict between the interests of the company and the nominator. In the event of a conflict, the nominee must either discharge their duty to the company and not to the nominator, or resign from the company's board.

The Corporations Act provides that directors appointed to the board of a wholly-owned subsidiary may act in the best interests of the holding company if certain conditions are satisfied and the constitution of the wholly-owned subsidiary expressly allows it.¹⁸

Alternate directors

Where directors find themselves unable to attend all board meetings or otherwise fulfil their board commitments, if the company constitution allows, then an 'alternate' director may be appointed. Depending on the scope of the appointment, the alternate director may exercise some or all of the appointing director's powers for a specified period. However, the appointment of alternate directors is becoming less common now that technology allows for participation in board meetings from a distance.

When an alternate director exercises the appointing director's powers, the exercise of powers is just as effective as if the power were exercised by the appointing director.¹⁹ The appointment process for alternate directors is typically governed by a company's constitution and is usually conditional upon board approval.²⁰

In the event that the appointing director has a conflict, the alternate (if exercising the appointing director's powers at that time) may still vote on the matter before the board. However, if the alternate also has a conflict then they must declare the conflict and refrain from voting.

The board should ensure that the terms of the appointment of an alternate director clearly set out:

- the scope of appointment (including any right to vote) and duration of the appointment
- the conditions under which the directorship may be revoked
- if the alternate director is permitted to attend all board meetings
- if there is an entitlement to receive all board papers and other communications.

De facto directors

A de facto director is a person not validly appointed as a director, but who by their actions is considered to in effect act in the position of a director. An example is where a person holds himself/herself out as a director by signing deeds as a director, despite not having a confirmation of appointment as a director, or not having been appointed in accordance with applicable procedures.

In practice, whether or not someone is deemed a de facto director will depend on the circumstances of each case, having regard to such factors as the size of the company, its internal structures and practices, and how the alleged director's position is perceived by outsiders who deal with the company.

Anyone deemed to be a de facto director is subject to the same duties and obligations as those applying to formally appointed directors, including the duty to prevent insolvent trading.

¹⁸ Corporations Act, 187.

¹⁹ Corporations Act, replaceable rule 201K.

²⁰ Corporations Act, 201K.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Shadow directors

A shadow director is a person who is not formally appointed as a director, but on whose instructions or wishes a company's directors are 'accustomed to act' as a matter of regular practice rather than as a one-off or isolated event.

A shadow director is subject to the same duties and obligations as those applying to formally appointed directors, including the duty to avoid insolvent trading.

A person will not be construed as a shadow director merely because the directors act on advice given by that person, due to their professional capacity or their business relationship with the directors. This is designed to protect lawyers, accountants, merchant bankers and others providing high-level advisory services to companies.

CHAIR'S ROLE

Just as the board sets the tone for the entire company, the chair sets the tone for the board. The chair is first among equals, leading by example, displaying the utmost professionalism and engaging in conduct that is beyond reproach. In this sense, it is difficult to imagine a well-performing board without an effective chair.

At its core, the chair's leadership role involves facilitating the effective contribution of all directors and promoting constructive and respectful relations between all directors and management.

An effective chair:

- demonstrates personal integrity through ethical behaviour and exercises power in the appropriate manner
- provides leadership by empowering and motivating board colleagues
- develops a positive relationship with the CEO and senior management
- commands respect by winning the confidence of fellow directors
- demonstrates strong communication skills, both verbal and written
- understands and demonstrates a commitment to corporate governance principles and practices

- operates as a team player, respecting, acknowledging and building on the views and perspectives of others
- promotes a suitable vision and strategy, offering strategic insight and direction
- oversees the development of a sound risk management framework.

The duties of the role and the personal characteristics and competencies required should be embodied in a chair's position description that is reviewed by the board on a regular basis.

As discussed before, to ensure a clear division of responsibilities at the head of the company, the ASX Principles recommend that the chair should be an independent director and that the respective roles of chair and CEO should not be exercised by the same individual.²¹ Further, for financial service companies that are required to comply with the regulations of the Australian Prudential Regulation Authority (APRA), under CPS 510, APRA mandates that the chair must be an independent director and cannot have been the CEO of the APRA-regulated institution at any time during the previous three years (although there are some dispensations for when the CEO position is unexpectedly vacated).²²

Similarly, the ASX Principles acknowledge the demanding and time-consuming nature of the chair's role.²³ This means that other commitments must not be allowed to detract from the chair's role.

The chair may be exposed to 'additional liability' where circumstances may arise that they are a recipient and 'gatekeeper' of information that may not be available to other directors. It is paramount to ensure that any significant performance shortcomings attributed to the CEO are brought to the board's attention and that the chair resists any complicity with the CEO to hold back information.

21 ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 2.5.

22 Australian Prudential Regulation Authority, Prudential Standard CPS 510 Governance

23 *ibid.*, Commentary to Recommendation 2.5.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

In addition, the chair must not prevent the CEO from raising issues with the board, nor should the chair fail to raise any matter that would reasonably be judged worthy of the board's consideration.

Given the significance of the chair's role, boards should give careful attention to the election of a chair. The common practice of electing a chair according to a notion of seniority should not be the default position. The role should be filled by the candidate best able to fulfil the duties referred to above.

DEPUTY CHAIR OR SENIOR INDEPENDENT DIRECTOR

Where the chair is not independent, it may be beneficial to consider the appointment of an independent director as deputy chair or as a 'senior independent director'.²⁴

The specific responsibilities of a senior independent director will vary among companies, but may include:

- acting as an intermediary between independent directors and the CEO, but not impeding opportunities for other directors to build constructive relationships with the CEO
- setting the agenda and briefing the CEO on issues arising from those sessions
- collaborating with the chair/CEO in the preparation of the board agenda and supporting papers
- acting as a sounding board for the CEO on issues where the CEO wants to 'test the waters' prior to raising an issue with the full board
- leading the appraisal of the chair/CEO
- providing a separate communication channel to the security holders (especially where those communications involve the chair).

The senior independent director is usually appointed by only independent directors, and a company's former CEO should not be appointed to this role.

²⁴ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 2.5.

COMPANY SECRETARY'S ROLE

The company secretary plays an important role in supporting the effectiveness of the board and its committees, including advising on governance matters.²⁵ As directors require more information, both in terms of quantity and quality, the company secretary fulfils an increasingly valued role, becoming a senior governance adviser to the board.

Both the Corporations Act and the ASX Principles state that the power to appoint and remove a company secretary should lie with the board.²⁶ The Corporations Act does not contain any general description of the role of the company secretary. It is a matter of the board's expectations of the person performing this role that will determine their ultimate responsibilities.

Company secretaries may have dual reporting lines if they hold multiple roles within the company.

The following general principles should apply to the company secretary's role:

- the company secretary is responsible to the board and should be accountable to the board through the chair on all governance matters
- the company secretary should report to the chair on all relevant matters relating to the board
- the company secretary's remuneration is usually approved by the board on the recommendation of the board remuneration committee
- a detailed position description for the company secretary should be prepared and approved by the board.

²⁵ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Commentary to Recommendation 1.4.

²⁶ Section 204D and 204F of the Corporations Act 2001 and Recommendation 1.4 of ASX Corporate Governance Principles and Recommendations (4th edition 2019).

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Company secretaries fall within the definition of a 'company officer' and essentially have the same legal duties and obligations as directors. It is increasingly common for company secretaries to perform a dual role (e.g. company secretary and general counsel), which has raised interesting issues regarding the extent of the application of the duty of care and diligence in section 180 of the Corporations Act, as was evidenced in the High Court's decision in the James Hardie case. The High Court in the decision against James Hardie's company secretary and general counsel, Mr Shafron, found that he was clearly an 'officer' and that his duties and responsibilities as general counsel and company secretary could not be divided or distinguished in the context of this matter.

The role of the company secretary may include:

- advising the board on corporate governance issues
- preparing the board agenda in consultation with the chair and CEO
- coordinating the timely completion and despatch of board papers
- ensuring that appropriate company records are maintained
- monitoring that board and committee policy and procedures are followed
- ensuring that the business at board and committee meetings are accurately captured in the minutes
- helping to organise and facilitate the induction and professional development of directors.

INDUCTION AND PROFESSIONAL DEVELOPMENT

Induction training and ongoing professional development for directors is critical to enable directors to effectively discharge their obligations.

ASX Principles Recommendation 2.6 indicates that a listed entity should have a program for inducting new directors and for periodically reviewing whether there is a need for existing directors to undertake professional development to maintain the skills and knowledge needed to perform their role as directors effectively.

It is important that induction training be comprehensive and commence immediately upon (if not prior to) the director's appointment, as director's liability and remuneration commences immediately.

Induction training should provide directors with an understanding of the entity's structure, operations, history and culture and involve appropriate site visits to key operations. Where gaps in directors' knowledge exist, induction training should be provided on key matters such as directors' legal duties and responsibilities under the relevant legislation governing the entity, and on key accounting matters and the responsibilities of directors in relation to the entity's financial statements.

Further, the ASX Principles recommend that companies should have and disclose a 'board skills matrix' setting out the mix of skills the board currently has or is looking to achieve.²⁷ A structured professional development program should be implemented that addresses gaps in directors' knowledge and skills as well as providing training in relation to emerging issues. The matrix should also be used in succession planning. In the consultation draft for a proposed fifth edition of the Corporate Governance Principles²⁸ the ASX are indicating that they may be looking for companies to disclose their process for assessing relevant skills and experience in the next iteration.

27 ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 2.2.

28 ASX, Consultation Draft for a proposed fifth edition of the Principles and Recommendations, <https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/corporate-governance-principles-and-recommendations-consultation-draft.pdf>

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- Australian Institute of Company Directors, Role of chief executive officer or managing director, <https://www.aicd.com.au/board-of-directors/roles/executive/role-of-chief-executive-officer-ceo-or-managing-director-md.html>
- Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, February 2019, <https://www.royalcommission.gov.au/sites/default/files/2019-02/fsrc-volume-1-final-report.pdf>
- IE University, CEO Duality: For Better and for Worse, <https://www.ie.edu/insights/articles/ceo-duality/>

For further information please contact:



Caron Sugars

**Lead Partner,
Board Advisory Services
KPMG Australia
ccobargsugars@kpmg.com.au**

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

3. Government

The roles, responsibilities and expectations of governing body members in the public sector differ in some respects from those of their corporate counterparts. Accountabilities also differ – the public interest, engagement with the community and the relationship with Ministers, Departments and Government are critical.

In this chapter

- Types of Government boards
- Roles
- Government is different
- Enabling Act for agencies
- Other legislation and policies
- Parent (or Lead) Department
- Appointment process
- Guidelines on caretaker conventions
- Acting in the public interest
- Community engagement
- Government engagement
- Strategic priorities
- Receiving assurance

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that directors of government entities should ask

1. Are governing body members well-versed in the enabling legislation that establishes the entity and defines their responsibilities?
2. Do all governing body members demonstrate a strong working knowledge of the agency's strategic priorities and how these align with whole-of-government direction?
3. Do members understand their obligations under relevant legislation (e.g. financial management, public administration, records management) and how these affect their compliance responsibilities?
4. Is there an effective framework for community engagement, and is the governing body ensuring the agency understands and responds to community needs and expectations?
5. Is the governing body aware of its duty to act in the public interest, and how that differs from private sector governance obligations?
6. Are governing body members fully aware of ethical conduct expectations in the public sector, including conflict of interest, privacy, integrity, and confidentiality obligations?
7. Are there strong working relationships between the agency and its relevant government departments or central agencies?
8. Does the governing body understand its accountability to government, the responsible Minister(s), and Parliament?
9. Are governing body members aware of restrictions on the use of public resources during election or caretaker periods to ensure political neutrality?
10. Is the governing body adequately informed about the broader policy, budget, and government priorities that may affect the entity's capacity to deliver on its objectives?

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The enabling legislation is never, or rarely, referenced in board papers, decisions, or governance documentation.
- Perceived or actual conflicts of interest are not disclosed or appropriately managed.
- The Chair does not engage regularly with the responsible Minister or the senior leadership of the entity's parent (or lead) department.
- The governing body receives a formal written direction from the Minister or government that overrides usual governance or decision-making practices.
- The Chair is not consulted or informed during the appointment or reappointment of governing body members.
- There is no structured approach or policy in place for engaging with the community.
- Governing body decisions do not consistently reflect the public interest or demonstrate ethical reasoning.
- A governing body member displays actual or perceived bias in favour of a stakeholder, lobby group, or political interest.
- Members accept gifts, benefits or hospitality in ways that are inconsistent with public sector or government policy.
- The governing body overlooks strategic priorities or fails to align agency decisions with Ministerial or government direction.
- Members demonstrate limited understanding of government funding mechanisms, appropriations, or budget accountability.
- There is no formal induction program provided to new governing body members by the agency and/or parent department.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

TYPES OF GOVERNMENT ENTITIES AND GOVERNING BODIES

Government entities come in many forms: statutory authorities, departments, corporations, commissions, advisory bodies, and more. These differences are not merely terminological; they reflect fundamental distinctions in structure, legal status, decision-making authority, and accountability mechanisms.

To simplify language in this chapter, we refer to all such organisations collectively as 'the agency.' Likewise, individuals who serve on the governance body – who may be called directors, members, commissioners, or committee members depending on the entity – are referred to as 'governing body members' for consistency and clarity. This chapter focuses on those bodies with formal governance and oversight roles, rather than purely advisory committees.

Important note: The type of entity (e.g. statutory authority vs. department) directly affects the extent of the governing body's authority, the independence of the agency, and its relationship to Ministers and departments. Governing body members must understand the nature of the entity they serve and the framework it operates within.

GOVERNMENT IS DIFFERENT

Governance in government is different. The diagram below highlights five key factors that set government agencies apart from their corporate counterparts:

	Organisational leadership	Often they don't have the authority to determine leadership of the organisation and appoint the CEO
	Community expectations	Stakeholders are wide and varied, with expectations from the community heightened for government agencies
	Not-for-profit motives	Agencies are not-for-profit motivated and are guided by the strategic direction set by government
	Political influence	Challenges that present governance in a political environment with influence in decision-making
	Funding constraints	Government agencies don't have continuous disclosure requirements, but must work within the funding constraints and timelines of government budget processes

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

JURISDICTIONAL DIFFERENCES

Each State, Territory, and the Commonwealth government has its own frameworks, legislation, and policy instruments governing public sector entities. While many governance principles are shared, requirements can vary significantly by jurisdiction. Governing body members must be familiar with the specific obligations relevant to their agency's location, funding model, and purpose.

At the federal level, many Commonwealth entities are subject to the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). This legislation sets out duties for accountable authorities, financial management obligations, and broader public sector values. However, not all federal bodies fall under the PGPA Act, and some are subject to other enabling legislation or hybrid arrangements.

UNDERSTANDING THE ROLE OF THE GOVERNING BODY

Governing body members in public sector entities have responsibilities that typically extend beyond those found in private companies. These may include formal obligations to:

- The Minister (or multiple Ministers, where applicable);
- The Parliament, either directly or indirectly (especially in relation to public reporting, budget use, and scrutiny); and
- The public, whose resources are being used and whose trust must be maintained.

In addition to oversight and strategic direction, some agency governing bodies are also tasked with providing policy advice to Ministers or Departments, or contributing to government policy development through the lens of operational experience.

Clarity is essential regarding the relationship between the Chair, the CEO, the Board, and the Minister. This is often defined (or at least influenced) by enabling legislation, conventions, and guidance issued by central agencies (such as DPCs or PM&C).

ENABLING LEGISLATION: THE FOUNDATION OF AUTHORITY

Most public sector agencies are established and governed by enabling legislation that outlines:

- The agency's purpose, functions, and powers
- The composition and responsibilities of its governing body
- Any specific reporting or oversight obligations

Governing body members should be thoroughly familiar with the agency's enabling Act and ensure that all decisions, processes, and delegations are consistent with its provisions. This includes understanding:

- Any provisions relating to the powers of the Chair, Minister, or Secretary
- Delegation frameworks and limits
- The agency's relationship to broader government machinery

OTHER APPLICABLE LEGISLATION AND POLICIES

In addition to the enabling Act, agencies are typically subject to a wide range of public sector legislation and policies, including but not limited to:

- Public sector ethics and integrity frameworks
- Financial management and budgeting legislation (e.g. Financial Management Acts)
- Freedom of Information, privacy, records management, and whistleblower protections
- Government procurement and advertising rules
- Public sector employment standards
- Sector-specific legislation (e.g. health, education, transport)

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Where the agency operates at the Commonwealth level, policies and directions issued by central agencies (such as the Department of Finance or PM&C) may apply, in addition to any formal Ministerial directions. These can, in some cases, override internal policy settings where permitted by law.

It is good practice for the agency to provide the governing body with a clear register or summary of applicable frameworks, including any specific departmental or whole-of-government policies that apply to it.

APPOINTMENTS TO THE GOVERNING BODY

Appointments to agency governing bodies are typically made by Ministers for a fixed term, and may be subject to legislative criteria, Cabinet approval, or other oversight processes depending on the jurisdiction. Appointment processes often include public advertisement and an assessment of candidates against published skills matrices or capability frameworks.

In some agencies, the Chair, CEO, or other governing body members may have input into the selection process or help identify suitable candidates, particularly where expertise or diversity is sought. Additional members may be appointed via elections (e.g. stakeholder-nominated members) or ex-officio positions linked to a role held in another organisation.

Governing body members should understand the formal process for appointments and reappointments in their jurisdiction and agency – particularly where delays or external dependencies (e.g. elections, Ministerial reshuffles) may affect continuity.

Selection criteria

Common criteria for appointment to public sector governing bodies may include:

- Personal integrity and standing in the community
- Legislative eligibility or mandated qualifications
- Understanding of public accountability and ethical decision-making
- Experience in governance, strategy, finance, law, policy, or the agency's sector
- Strategic thinking and long-term planning skills
- Knowledge of government systems and policy cycles
- Familiarity with the agency's key risks, stakeholders, and service delivery context
- Intergovernmental or stakeholder relationships
- A commitment to diversity and inclusive representation
- Capacity to attend and actively participate in meetings

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ELECTIONS AND CARETAKER CONVENTIONS

When a general election is officially called, the Government enters a caretaker period, during which major decisions are deferred to avoid unduly binding an incoming administration.

Recently, the Commonwealth Government issued a refreshed version of its formal 'Guidance on Caretaker Conventions', which is largely consistent with prior guidance but updated in formatting and accessibility.¹ These refreshed guidelines reaffirm that the conventions:

- Are not legally binding; their application requires judgment and common sense, and they are applied consistently across agencies
- Take effect from issuing of writs until either the election outcome is clear, or if government changes, until the new government is appointed by the Governor-General

During the caretaker period:

- Agencies should avoid major policy decisions, new significant appointments, and committing to substantial contracts or undertakings unless they are urgent and, often, subject to consultation with the Opposition
- Appointments and reappointments to governing bodies are commonly paused or deferred, with any necessary appointments capped in duration (e.g. short-term or acting) or subject to consultation
- Public communication and campaigns must remain apolitical. Agency websites and social media should restrict new content that could be interpreted as partisan. Routine or factual updates related to essential services may continue with caution
- Public servants continue routine administration, but must strictly avoid activities that could benefit a political party, including through use of government resources

Governing body members should:

- Ensure they understand the relevant caretaker guidelines for their jurisdiction, including any recent updates (e.g. Commonwealth's 2025 Guidance).
- Plan for potential delays to appointments, contracts, policy approvals, or engagements requiring Ministerial sign-off.
- Confirm that public communications, stakeholder engagement, or decisions align with caretaker norms around neutrality and restraint.

ACTING IN THE PUBLIC INTEREST

Unlike corporate governance, where directors act primarily in the best interests of the company, governing body members of public entities must act in the public interest – balancing stewardship of public resources with ethical obligations to the community. This includes:

- Complying with public sector codes of conduct and values
- Demonstrating integrity in all decision-making and delegations
- Upholding transparency and accountability
- Promoting efficient and ethical use of public funds
- Managing conflicts of interest appropriately
- Escalating suspected misconduct, corruption, or maladministration
- Respecting restrictions on gifts, hospitality, or personal benefit

Public trust is a core asset of any government agency. Governing body members should model the highest standards of ethical behaviour – not only to comply with law and policy, but to uphold confidence in government institutions more broadly.

¹ <https://www.pmc.gov.au/resources/guidance-caretaker-conventions>

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

COMMUNITY ENGAGEMENT

Effective governing body members understand the value of genuine community engagement – both as a source of insight and as a means of legitimacy. Agencies may engage communities through:

- consultation forums, workshops, and roundtables
- attendance at public events and agency-run outreach
- targeted engagement with specific communities, sectors, or priority groups
- digital feedback platforms or structured research.

Governing body members should ensure the agency has an appropriate community engagement strategy or policy in place, particularly where community expectations, equity considerations, or service design are central to the agency's role.

GOVERNMENT ENGAGEMENT

Governing body members must also understand how their agency engages with Ministers, departments, and central agencies. Unlike corporate boards, which operate independently from shareholders, public sector boards often sit within a web of government relationships and layered accountability. Key considerations include:

- clarifying who can speak to government and on what matters
- ensuring consistency of communication across the agency
- having protocols or policies that manage engagement and reporting
- understanding the agency's place within broader strategic, policy, and budget cycles.

A well-governed agency is one that communicates transparently and proactively with its Minister and lead department – without drifting into advocacy, partisanship, or operational micromanagement.



Case study: Queensland Health

The report titled 'Fraud, financial management and accountability in the Queensland public sector' provides a detailed account of the fraudulent activity that took place at Queensland Health (QHealth) by an individual employee which resulted in a series of 65 fraudulent transactions, totalling \$16.69 million, committed over a four year period from 2004–2011. The report includes key learnings for the general application across the public sector, focusing on high risk employees and internal control weaknesses that place an agency at risk.

Recommendations resulting from the example:

Management should increase vigilance in the following five main areas:

1. Financial management
2. Managerial standards and accountability
3. Acceptance of gifts and benefits
4. Managing risk in a context of organisational change
5. Fraud awareness and prevention

Additionally, it is recommended that agencies consider and address these issues in all levels of their organisation including, but not limited to, executive management, with particular consideration by members of risk and audit committees. All managers and supervisors are encouraged to regularly review their internal processes and practices in order to identify any emerging issues.

The full report can be found at [Fraud, financial management and accountability in the Queensland public sector: An examination of how a \\$16.69 million fraud was committed on Queensland Health | CCC - Crime and Corruption Commission Queensland](#).

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US



Case study: Department of Communities (Western Australia)

In November 2021, Paul Whyte was jailed for 12 years after defrauding the government of \$27 million between 2008 and 2019. It was reported in court that Mr Whyte approved fictitious invoices and credit card transactions which resulted in payments to three companies owned by a co-accused who was a personal friend of Mr Whyte's. Police were able to uncover how some of these funds ultimately were used to pay Mr Whyte's mortgage.

In addition, payments were made to a company, Ausmodular, owned by another co-accused for construction of a camp where no work was performed. This money was extracted by Mr Whyte's brother through invoices submitted to Ausmodular with the funds being used to buy a house in a luxury suburb in Mr Whyte's wife's name.

The judge, Justice Joe McGrath, made the point that there was a failure of the public service to have the appropriate controls in place to prevent and detect the fraudulent activity that Mr Whyte engaged in and as he held a senior role, he was aware of these weaknesses and exploited them for his own benefit.

The Corruption and Crime Commission stated that 'In short, Mr Whyte was the ideal public servant. Except it was all a lie'.² He was uncovered after they received information that suggested 'conduct associated with questionable behavioural and lifestyle habits'.³

Auditor-general Caroline Spencer described that whilst fraud involving collusion can be difficult to detect, she 'wanted good management controls, robust internal audit functions and audit committees which followed up on recommendations.' and that 'segregation of duties and rotation of duties within public agencies was also important'.⁴

The CCC's full report can be access here: [Exposing Corruption in Department of Communities.pdf](#)

² Ramsey, M. (2021), The Western Australian, <https://www.perthnow.com.au/news/court-justice/wa-bureaucrat-epitome-of-corruption-c-4581797>

³ ibid

⁴ Weber, D. (2019), ABC News, <https://www.abc.net.au/news/2019-11-21/paul-whyte-department-communities-fraud-not-detected-auditing/11726292>

STRATEGIC PRIORITIES AND ALIGNMENT

In the public sector, strategy doesn't exist in a vacuum. Government agencies operate within a strategic direction set by the elected government, and are typically expected to align with whole-of-government priorities, Ministerial directions, and broader sector reforms. Governing body members should:

- understand the government's strategic intent and how it applies to their agency
- ensure the agency's corporate and strategic plans reflect this direction
- monitor progress using clear performance indicators and accountability mechanisms
- challenge management to be responsive to changes in public expectations or political priorities.

Strategic priorities commonly include:

- long-term planning for resilience, sustainability, and service delivery
- responsiveness to emerging risks, stakeholder feedback, and community needs
- clear links between funding, delivery, and performance outcomes
- transparent reporting on progress, setbacks, and value for money.

This balancing act – between independence in operations and alignment with government policy – is a defining challenge of public sector governance.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ASSURANCE, OVERSIGHT, AND INTEGRITY BODIES

Public sector agencies operate within a distinct assurance ecosystem that includes formal audit and investigative bodies. These provide independent scrutiny and are often accountable directly to Parliament, rather than government. Key players include:

- Auditor-General (State or Commonwealth): Responsible for performance and financial audits, and ensuring agencies are delivering on their mandates efficiently and lawfully.
- Ombudsman: Investigates complaints and systemic issues within public services. Often has broad powers to examine administrative fairness, service delivery, and maladministration.
- Anti-corruption bodies or integrity commissions: In many jurisdictions, specialist bodies investigate serious misconduct or corruption within government entities.
- Central agencies: Departments of Premier & Cabinet, Treasury, or Finance often issue standards and conduct compliance reviews.

Governing bodies should:

- establish strong internal audit and risk functions, typically via an Audit and Risk Committee
- regularly review compliance with legislative obligations and public sector policies
- monitor follow-up on audit recommendations, Ombudsman findings, and integrity reviews
- foster a culture of openness, defensible decision-making, and ethical leadership.

Governing body members don't need to 'audit the auditors' – but they do need to understand where assurance is coming from, what gaps may exist, and how the agency responds to scrutiny.



FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- Australian National Audit Office, Audit Insights: Board Governance, 2019, <https://www.anao.gov.au/work/audit-insights/board-governance>
- Australian National Audit Office, Effectiveness of Board Governance at Old Parliament House, April 2019, <https://www.anao.gov.au/work/performance-audit/effectiveness-board-governance-old-parliament-house>
- Australian National Audit Office, April 2019, Effectiveness of Board Governance at the Australian Institute of Marine Science, <https://www.anao.gov.au/work/performance-audit/effectiveness-board-governance-the-australian-institute-marine-science>
- Australian National Audit Office, May 2019, Effectiveness of Board Governance at the Sydney Harbour Federation Trust, <https://www.anao.gov.au/work/performance-audit/effectiveness-board-governance-the-sydney-harbour-federation-trust>
- Victorian Government, Victorian Public Service Commission, <https://vpssc.vic.gov.au/#board-members>
- NSW Government, Senior Executive Fundamentals, <https://sef.psc.nsw.gov.au/understanding-the-sector/boards-and-committees>
- Government of South Australia, Department of Premier and Cabinet, *Government Boards and Committees, Guidelines for Agencies and Board Members, 2000* <http://dpc.sa.gov.au/documents/rendition/B17636>
- Government of Western Australia, Governance of WA government boards and committees www.wa.gov.au
- The Department of Finance (Cth) has published the following guidance relevant to GBEs: *Resource Management Guide No. 126 – Commonwealth Government Business Enterprises – Governance and Oversight Guidelines*. Refer to: [Government Business Enterprises \(GBEs\) \(RMG 126\) | Department of Finance](#)

For further information please contact:



Elise Wherry

**National Industry Lead,
Infrastructure, Government and Healthcare
KPMG Australia
ewherry@kpmg.com.au**

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

4. Not-For-Profit Organisations

The roles, responsibilities and expectations of directors of Not-For-Profit (NFP) organisations are inherently the same as those of their corporate and government counterparts. Key differences exist, however, with respect to aspects of legal compliance, tax obligations, strategic and operational areas of focus and accountability to members.

In this chapter

- Directors' legal responsibilities
- Structuring an effective NFP board
- NFP leadership
- Strategic priorities
- Stakeholder engagement
- Identification, management and mitigation of risk
- Receiving assurance

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that an NFP director should ask

1. Are all directors well-versed with the constitution and rules of the board?
2. Do all directors understand their responsibilities relating to the Constitution, related government legislation and tax compliance?
3. Does each board member display strong working knowledge of the strategic priorities?
4. Are directors taking steps to engage with members and understand expectations?
5. Is the board aware of its duty to meet the objectives and vision of the organisation?
6. Are all directors fully aware of their duties and responsibilities regarding conflicts of interest?
7. Is there an effective framework for membership/ constituent engagement?
8. Are there strong working relationships across the organisation with members and stakeholders (including government departments for government boards)?
9. Is the board's role with members and the services provided to members well understood?
10. Do directors recognise the importance of ethical conduct in the NFP sector?

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The mission or purpose of the organisation is ambiguous, and never, or rarely, referred to in board discussions/documentation.
- There is no discussion of risk.
- There is no regular and/or accurate presentation of results or forecast cashflows.
- Certain directors are perceived to have conflicts of interest.
- There is concern that participation and engagement with members is poor.
- The directors fail to act in accordance with the objectives/purpose of the organisation.
- The board, or certain directors, do not invest sufficient time on governance of the organisation.
- A director is demonstrating strong bias towards lobby groups (or similar) within its membership.
- The board ignores its strategic priorities in its decision-making framework.
- Directors display lack of understanding of NFP organisation's funding and compliance obligations.
- Some directors are on the board for many years.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

NFP entities are organisations that exist for 'public benefit', whereby their key objective is to provide a range of community services or advocacy activities (such as health, education, counselling or spiritual guidance, lobbying or improving the environment) for the communities they serve. Ensuring the ability to deliver these services to their communities over time, means that being financially viable is important. The key difference between a corporation and an NFP entity is that any profits are applied by the NFP entity to fulfil its overall purpose, rather than generating gains or benefits for distribution to members.

Setting and understanding the overall objective, vision, mission and values of an NFP entity is critical to establishing the context of its operations and the strategic focus of the board.

This section focuses on key differences that directors of NFP entities need to be cognisant of and be able to manage effectively. For clarity, this section does not specifically cover government entity boards as this is covered in [Chapter 3 Government](#).

DIRECTORS' LEGAL RESPONSIBILITIES

NFP legal structures

It is important to recognise that there are many different types of NFP organisations, each one with a unique set of legal obligations, tax obligations, regulators and reporting requirements. In developing this chapter, we have focused on general observations applicable to NFP entities more broadly, however, there may be specific considerations that are applicable to your NFP entity. As a director of an NFP entity, you must pay careful attention to the legal structures under which the NFP entity operates and ensure that independent professional advice is sought with respect to your duties and responsibilities within your organisation.

NFPs may be referred to as an 'association', 'college', 'club', 'company', 'foundation', 'fund', 'institute', 'league', or 'society'. The classification is determined largely by the legal structure under which the organisation is established and whether the organisation is a registered charity, which in turn, will impact on its tax status.

Throughout this chapter, we will refer to the NFP organisation as 'the NFP entity' and the governance representation as the 'NFP entity board'. You may be called a director, member, councillor or committee member and we will refer to you as a 'director' through this chapter.

The legal structure used to establish the NFP entity will determine the various financial, operational and compliance functions of the board. In addition to the legal duties outlined in [Chapter 1 Directors' Legal Duties](#), the different legal structures applicable to NFP entities, means that directors must invest time in understanding the relevant laws and the associated legal, operational, financial (e.g. tax exemptions) and reporting requirements in order to effectively fulfil their duties.

Some of the more common legal structures include:

- Companies limited by guarantee
- Incorporated Associations
- Unincorporated Associations
- Co-operatives
- Indigenous Corporations
- Gift Funds
- Trusts
- Trade Unions
- Entities created by Acts of Parliament ('creature of statute')
- Federated models.

A significant number of NFP entities are established as either an incorporated association or a company limited by guarantee.

Incorporated associations are legal entities separate from its individual members and are subject to the relevant state or territory legislation in which they operate. This means that the majority of their operations tend to be restricted to that jurisdiction. The liabilities and financial protections of the entity are limited.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Companies limited by guarantee are governed by the *Corporations Act 2001* (regulated by ASIC). NFP entities established under this legal structure are public companies, and the liabilities of the company members are also limited to the extent of the guarantee.

Some key considerations for NFP entities in determining the most appropriate legal structure are:

- Where will the non-profit operate?
- Will there be changing membership?
- What is the nature of the activities?
- How will the organisation raise money?

As noted above, NFP entities and individual directors should seek specific advice from a professional adviser with respect to legal, tax or accounting matters, prior to implementing or affecting changes to the NFP entity's legal structure.

Charitable NFPs

Not all NFPs are charities, however, under Australian law, all charities must be an NFP. The *Charities Act 2013* (Cth)¹ defines an entity as an NFP entity that serves 'for the public benefit'. Being a registered charity allows NFPs to receive certain tax concessions from the ATO and, therefore, is regulated by a national regulator, the Australian Charities and Not-for-profits Commission (ACNC).

With respect to discharging their legal duties, directors of charitable NFPs have an additional duty to ensure that they dutifully oversee how members' funds, assets, and products and services are managed to meet their community's needs. Therefore, the support of the charitable NFP entity in the maintenance of 'public benefit', or its mission, is key.

As such, in the duty of public benefit, directors should give consideration to the following:

- compliance with the relevant NFP ethical frameworks
- compliance with the defined values and standards generally outlined in the NFP's code of conduct
- ensuring a full understanding of the organisation's legal obligations and director's individual responsibilities
- acting with integrity and ensuring ethical decision-making occurs across delegated powers in favour of public benefit
- compliance with NFP, financial, asset management and procurement requirements, in addition to conscientious expenditure of membership funds
- awareness and declarations of all conflicts of interest
- escalation of identified or suspected corruption
- attentiveness to the illegality of acceptance or offering of gifts or rewards.

¹ Charities Act 2013, <https://www.legislation.gov.au/Details/C2013A00100>

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Tax concessions for NFPs

The ATO can provide tax concessions (including income tax, FBT concessions/exemptions and deductible gift recipient status) to certain types of NFPs (including registered charities, health organisations, community service organisations etc.), but only where its constituent or governing documents explicitly state that profits or assets are prevented from being distributed for the benefit of particular individuals (i.e. owners, shareholders) – both while it is operating and when it winds up.

NFPs that are registered charities with the ACNC must go through an endorsement process with the ATO. The tax concession application process forms part of the application to become a registered charity with the ACNC and is submitted by the latter to the ATO to assess eligibility. Other NFPs do not require this endorsement and can become income tax exempt through a self-assessment process outlined by the ATO. Additional tests and rules, including annual reviews to determine ongoing eligibility apply.

Regulation of charitable NFPs

For entities that are registered charities (under the *Charities Act 2013*), there are also additional obligations that are regulated by the ACNC.

Established in 2012, the ACNC actively monitors and engages with charitable NFPs to ensure ongoing compliance with the conditions for maintaining charitable status through ensuring that the charity is:

- working towards its charitable purpose
- using its profits and assets only for its charitable purpose
- meeting its reporting obligations
- meeting its records keeping obligations
- meeting the ACNC Governance Standards.²

ACNC Governance Standards

Charities are required to meet a minimum set of governance standards that are set out by the ACNC. Failure to meet these standards puts the charitable NFP at risk of losing its charitable status, which can have significant financial, tax and reputation impacts. Standard 6 was added in February 2021 with the purpose of maintaining and enhancing public trust and confidence in the Australian charity sector by ensuring that a registered charity's governance enables it to be accountable for its past conduct relating to institutional child sexual abuse.

² Refer to ACNC Governance Standards, <https://www.acnc.gov.au/for-charities/manage-your-charity/governance-hub/governance-standards>

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ACNC Governance Standards

**Standard 1 – Purpose and not-for-profit nature**

Charities must be not-for-profit and work towards their charitable purpose. They must be able to demonstrate this and provide information about their purposes to the public.

**Standard 2 – Accountability to members**

Charities that have members must take reasonable steps to be accountable to their members and provide them with adequate opportunity to raise concerns about how the charity is governed.

**Standard 3 – Compliance with Australian Laws**

Charities must not commit a serious offence (such as fraud) under any Australian law or breach a law that may result in a penalty of 60 penalty units (equivalent to \$12,600 as at December 2018) or more.

**Standard 4 – Suitability of Responsible Person**

Charities must take reasonable steps to:

- be satisfied that its Responsible Persons (such as board or committee members or trustees) are not disqualified from managing a corporation under the *Corporations Act 2001* (Cth) or disqualified from being a Responsible Person of a registered charity by the ACNC Commissioner, and
- remove any Responsible Person who does not meet these requirements
- ensure that the charity's financial affairs are managed responsibly
- not allow a charity to operate while insolvent.

ACNC Governance Standards (continued)

**Standard 5 – Duties of Responsible Person**

Charities must take reasonable steps to make sure that Responsible Persons are subject to, understand and carry out the duties set out in this Standard:

- act with reasonable care and diligence
- act honestly and in the best interests of the charity and its purpose
- not misuse the position of responsible person
- not misuse information obtained in performing duties
- disclose any actual or perceived conflict of interest
- ensure that the charity's financial affairs are managed responsibly
- not allow a charity to operate while insolvent.

**Standard 6: Maintaining and enhancing public trust and confidence in the Australian not-for-profit sector**

Charities must take reasonable steps to become a participating non-government institution if the charity is, or is likely to be, identified as being involved in the abuse of a person either:

- in an application for redress made under section 19 of the *National Redress Scheme for Institutional Child Sexual Abuse Act 2018* (Cth) (Redress Act), or
- in information given in response to a request from the National Redress Scheme Operator (Secretary of the Department of Social Services) under section 24 or 25 of the Redress Act.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The AICD have also published the 'Not-for-Profit Governance Principles' (April 2024).³ The guide contains 10 key principles that cover similar concepts as those outlined in the Corporations Act, with specific tailoring for the NFP sector. The principles are:

1. Purpose and strategy
2. Roles and responsibilities
3. Board composition
4. Board effectiveness
5. Risk management
6. Performance
7. Accountability and transparency
8. Stakeholder engagement
9. Conduct and compliance
10. Culture

Directors must ensure that they are aware of all of the requirements of legislation governing charitable NFPs, remembering that in essence the obligations are the same as a 'for profit' entity, with the addition of ensuring (and demonstrating) that the 'public benefit' continues to be met.

Applicability of the Corporations Act 2001

To reduce any misalignment between the governance requirements of the Corporations Act and the ACNC Governance Standards, the following Corporations Act requirements are not applicable for NFP entities registered under the ACNC Act. Instead, registered charities are required to take reasonable steps to ensure that any responsible persons comply with Governance Standard 5.⁴

Provisions that no longer apply	Summary of provisions
Directors duties	
sections 180 to 183; and section 185, to the extent that it relates to sections 180 to 183	Civil obligations of directors and other officers to: – exercise due care and diligence – act in good faith – not improperly use their position, and – not improperly use company information
section 188, to the extent that it relates to another provision mentioned in this table	Responsibilities of secretaries and directors for certain contraventions
section 191 – 194	Interests of directors
Additionally the following provisions of the Corporations Act are not applicable, as they are replaced by provisions from the ACNC Act:	
Corporate reporting	
subsection 136(5)	Public company must lodge with ASIC a copy of a special resolution adopting, modifying or repealing its constitution
section 138	ASIC may direct company to lodge a consolidated constitution

3 Refer to AICD Not-for-Profit Resource Centre, <https://www.aicd.com.au/corporate-governance-sectors/not-for-profit/studies/2024-not-for-profit-governance-principles.html>

4 ASIC, Corporations Act provisions that no longer apply to charities registered with the ACNC, refer to <https://asic.gov.au/for-business/running-a-company/charities-registered-with-the-acnc/corporations-act-provisions-that-no-longer-apply-to-charities-registered-with-the-acnc/>

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Provisions that no longer apply	Summary of provisions
section 139	Company must send copy of constitution to members
subsection 142(2), section 146 and subsection 146A(2)	Company must notify ASIC of changes of address
section 201L and 205A to 205C; section 205D, to the extent it relates to section 205B and section 205E	Public information about directors
Chapter 2N	Updating ASIC information about companies and registered schemes
Part 2G.2 (other than sections 250PAA and 250PAB); and Part 2G.3, to the extent that it relates to meetings of the body corporate's members	Meetings of members
Parts 2M.1 to 2M.3	Financial reports and audit
sections 601CDA, 601CK and 601CTA	Foreign companies
subsection 601CT(3), section 601CV and subsection 601DH(1) to (1A)	Registered body must notify ASIC of certain changes

Other legislation

Whilst this chapter contains an overview of key principles relevant to directors of NFP entities and charitable NFPs, it is important to note that every jurisdiction has different requirements, guidelines and legislation.

Other regulators include the Office of the Registrar of Indigenous Corporations (ORIC) and the Australian Taxation Office (ATO).

A list of regulators that may affect NFP entities can be found on the Australian Charities and Not-for-Profit (ACNC) website (<https://www.acnc.gov.au/list-regulators-may-affect-charities>)

Similarly, overarching legislation and regulations such as privacy, equal opportunity, freedom of information, environmental protection, occupational health and safety and fair trading laws apply equally to NFPs as they do to 'for profit' entities. These are discussed in more detail in [Chapter 1 Directors' Legal Duties](#).

Each director must invest time in understanding the relevant laws that bind their specific association and the impact on their obligations.

Changes to reporting obligations for charities

The ACNC have reduced the reporting thresholds for charities⁵ so that fewer charities will need to produce financial reports and can rather complete an Annual Information Statement instead. In addition, the changes enable smaller charities to elect for a review rather than an audit of their financial reports.

From 2022, when charities complete their Annual Information Statements, the thresholds for determining whether a charity is small, medium or large for financial reporting purposes will change to those shown below.

⁵ ACNC, January 2022, Upcoming changes to charity size thresholds are good news for charities, refer to www.acnc.gov.au/media/news/upcoming-changes-charity-size-thresholds-are-good-news-for-charities

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Size of charity	Revenue thresholds for Annual Information Statements	Audit/review requirement
Small	Less than \$500,000	Only have to complete their Annual Information Statement online.
Medium	\$500,000 – \$2,999,999	Financial report can be either reviewed or audited.
Large	\$3 million or more	Financial report must be audited

STRUCTURING AN EFFECTIVE NFP BOARD

Depending on the constitution of the entity, boards may be elected by members, or appointed through a competitive selection process. Depending on the constitution, some boards may be comprised solely of members whilst others may allow for some independent directors so as to expand the skills of the board.

Where the NFP has adopted a federated structure, coordinating any number of component bodies (often state-based with a national body at the top), a board of the top (potentially national) entity will be responsible for oversight of the individual component bodies as well as the stewardship of one single federated body. To ensure appropriate representation, boards of the overall federated body typically comprise representatives (also called nominees) from each of its component bodies.

Though this model presents some clear strengths, it is becoming more common to include one or more independent directors (and especially an independent chair) on the federation board, where the constitution allows. This helps to protect and promote the necessary balance in focus between maintaining oversight of the individual component bodies and guiding the overall strategic direction of the federated organisation.

Appointment process

Members generally vote to make appointments to NFP boards for a fixed term. Whilst not always the case, the appointments are generally advertised to members via public media, which outline the core skills and competencies required. The board chair, CEO and NFP entity members may in some cases select 'public members' to the board, or there may be a Nominations Committee as part of the board governance structure, that has been established specifically to address board appointments. Public members are selected to address board skills deficits or to balance elected board member composition (gender, experience and qualifications, geographical) through an expression of interest. Existing directors and the chair can help to create a pool of potential candidates through continuous networking as a form of succession planning. In some cases, there may be a combination of member elected board members and board appointed directors, to achieve a balance between member representation and ensuring the appropriate skills are in place. Further entity appointments can occur via elections, ex-officio 'requirements', expressions of interest, nominations for improved NFP entity composition, and reappointments.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Criteria for selection

The selection criteria used by NFP entities to elect and/or appoint board members and a chair may include, but is not limited to:

- the status and integrity of the individual within the community (membership) in which they work
- adherence to the duties of a non-executive director with reference to the Corporations Act, if applicable
- any other legislative requirements applicable to that board (e.g. mandatory governance requirements of other commissions)
- working knowledge and understanding of accountability relationships
- relevant experience within the sector and their elected field(s) of excellence
- ability to think and act strategically
- understanding of the NFP organisation and sector operations
- understanding of the objectives and role requirements of their position
- existing relationships and connectivity
- understanding of the key risks and challenges present in the NFP sector
- governance standards understanding
- capacity to contribute (in time and often financially) and attend board and subcommittee meetings.

To achieve a 'balance of expertise' on an NFP board, there may be a greater need to consider, and give heavier weight to, the candidate's corporate business and financial expertise, advocacy or stakeholder engagement.

Sourcing

Strategic workforce planning at a board level should be informed by board evaluation and completion of skills matrices to highlight gaps and drive selection based on 'public member' candidate expertise. Embedded in this is the management of talent identification and due diligence.

Probity considerations that should be taken into account when sourcing and selecting candidates may include, but are not limited to:

- proof of identity checks
- verification of qualifications
- ASIC registration/disqualification check
- working with children check
- police/criminal record check
- declaration of private interests/conflict of interests
- personal reference checks.

Depending on the jurisdiction in which the NFP entity operates, these requirements may differ.

Director resignation, retirement and removal

Director involvement on NFP boards can often be driven by personal values or connections to the organisation. Sometimes, however, despite this passion and commitment, the director does not have the skills or experience required to operate effectively on the board. Other issues associated with board renewal in the NFP sector include board members who – due to constitutional limitations or other reasons, like a sense of obligation – have remained on the board for many years, thereby limiting options for new members to join and bring a fresh perspective. This can create significant issues with respect to the ability of the board to fulfil its legal and governance duties. This is where a clearly defined board governance framework, including clearly documented appointment processes, tenure, skills requirements and performance measures of directors is critical.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Removing a director in these types of sensitive situations can be challenging. The options available will depend on the legal structure of the NFP entity. For example, an NFP entity may be able to move the director to a subcommittee (e.g. fundraising) to focus their effort on a specific function to which they feel strongly connected and to which they can make a more significant contribution, but they cannot do this if they are a company limited by guarantee. Directors of NFP entities operating as companies limited by guarantee can often only be removed by a member vote.

Challenges of finding and retaining NFP directors

Directors of NFP entities are often unpaid. The AICD's 2023-24 *Not-for-Profit Governance and Performance Study*⁶ found that only 21 percent of respondents were remunerated, however, this varies by sector.

In addition, the survey also found that half of respondents report their time spent on their director role is somewhat more or twice as much (37 percent and 13 percent respectively) compared to last year.⁷

Finding candidates who are willing to invest the time and effort in a 'volunteer' role with such high levels of responsibility and accountability can often be challenging. Conversely, some NFPs find that directors join with great passion and intent for the purpose, but do not have strong governance skills, especially when NFP boards are often the first governance role for individuals looking to gain governance experience in an unlisted and 'less high profile' environment. The reality is that the expectations, accountabilities and obligations are inherently the same for NFPs as for 'for profit' entities.

NFP LEADERSHIP

The relationship between CEO and the board is a critical one for NFPs. Unlike other organisations where the CEO reports to the board, often in NFPs, the CEO is a key resource for directors – providing assistance in:

- assisting directors (who are often volunteers) to understand their duties
- making recommendations for board recruitment that align with the NFP entity's culture and skill needs
- increasing the awareness of directors about the organisation's objectives and programs
- participating in strategy development and board committees.

It is critical that CEOs and NFP directors have an effective working relationship that is based on shared objectives, open communication and a strong understanding and respect for each other's role and skills.

Within NFPs, the line between board and management can be less clear than in private organisations (especially listed companies). Resource constraints can often mean that directors are required to get more involved in operational issues, thereby stepping out of their oversight role and into implementation – i.e. less 'steering' of the boat and more 'rowing'.

Again, in these instances, it is critical for the board to recognise and clearly define when it is required to move into operational matters. Whilst the Board Charter is an important document to define the role of the board (and all NFPs should have a clearly documented Board Charter), the Delegations of Authority (DoA) is critical to explicitly define how board and management interact, and the levels of responsibility for decision-making with respect to implementation of the NFP's mission and strategy.

⁶ AICD 2023-2024, Not-for-Profit Governance and Performance Study, refer to <https://www.aicd.com.au/content/dam/aicd/pdf/news-media/research/2024/nfp-governance-performance-study-2023-24-web.pdf>

⁷ *ibid.*

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

STRATEGIC PRIORITIES

Like corporate boards, the overall strategic framework, direction and priorities for an NFP entity are set by the board. NFP entities should set their strategic priorities within this framework and be consistent with the board's direction. It is the duty of a director to ensure that they are familiar with the mission and strategic priorities of the entity. The NFP's CEO should oversee the alignment of the mission with its strategic direction and operational activities.

Part of the development of strategic priorities requires a clear understanding and agreement on the mission or objectives of the NFP entity. Membership-based associations may be motivated by public benefit, prestige and advocacy within the industry, and the relationships between members and stakeholders. In contrast, other NFPs (health and education services) may be motivated by achieving the best possible health, education and/or wellbeing outcomes for the communities that they support.

Types of issues specific to NFPs and the development of strategic priorities are detailed below.



Case study: The Returned and Services League of Australia (NSW Branch)

In February 2018, the NSW Government released the findings of an inquiry into the financial and fundraising activities of RSL NSW. The inquiry was commissioned as a result of concerns regarding *RSLs compliance with the NSW Charitable Fundraising Act 1991 (NSW)*, specifically with respect to how funds raised were used by the organisation, with concerns that funds were not being used for a charitable purpose.

The NSW state branch was rocked in late 2016 by revelations that the State President (and director) had spent \$475,000 on a corporate credit card over a six-year period, including \$213,000 in cash withdrawals.

There were further allegations of \$150,000 of spending by the director that was not accounted for with receipts; the use of an RSL NSW credit card to fund his son's use of a presidential suite at a Sydney hotel over a period of seven years; and the use of the RSL NSW credit card to cover mortgage repayments, flights for family and meals over an 11 year period. In addition, some board members, including the State President and former National RSL President, received tens of thousands of dollars a year in 'consulting fees' from the league's aged care arm, RSL LifeCare.

The inquiry undertaken by Supreme Court Judge Patricia Bergin, identified a number of areas of director financial misconduct, and recommended that the former RSL NSW President be referred to police over misuse of credit cards.

The high-level inquiry also recommended:

- thirteen directors be referred to charity watchdogs in connection with the cover-up of expenses
- eight board members and executives of the aged care arm be referred to the watchdogs in connection with payments made to some voluntary board members that appeared to breach charities regulations.

The importance of purpose

The foundation of the NFP entity's governance framework is its constitution. This legal instrument defines the organisation's mission, purpose, objectives, general powers, functions and duties, and the responsibilities of its directors. The constitution should clearly outline the entity's legal structure, charitable/non-for-profit status and governing laws.

The directors should be well versed with the constitution and review all NFP entity instruments, processes and functions against it.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

A key component of the constitution is to define the organisation's mission and purpose. Critically, for NFP entities, the alignment of activities with its mission can be challenging. In some instances, social drivers (such as increasing demand for diversified services), resource/skills constraints and funding pressures can move organisations away from their mission, thereby creating unique risk and strategy issues for directors.

For example, NFPs often generate 'revenue' through donations or grants. In the case of grant funding, money is often provided to meet specific government policy objectives. In some cases, these objectives will broadly align with the organisation's mission, however may require the NFP to direct some of the resources into other related but non-core services. Over time, these 'new' services can move the organisation into areas that do not fully align with the NFP's mission.

In this instance, risk and strategy issues can arise that might put the organisation into conflict with itself. For example, an NFP established to provide assistance to low income households may receive funding to retrofit households with energy efficient light bulbs (reducing energy bills for low income earners). Whilst in alignment with the NFP's mission, it may require specialist skills with respect to installation of equipment or electrical modifications within a home. Whilst the funding would no doubt assist the NFP achieve its mission, it comes with a range of legal, operational and reputational risks that need to be considered. Pursuing this service offering could distract the organisation from its core purpose and further constrain the use of scarce resources.

Directors, therefore, need to understand the range of risks that these opportunities can present (particularly in a competitive funding environment). This requires a thorough understanding and oversight of risk management practices within the organisation.

Governance roles are also characterised by the size and nature of the organisation and its scope of operations. For example, larger NFP entities operating multimillion dollar budgets and operating at a national scale will have vastly different governance requirements than a community sporting club.

Managing funding constraints

NFPs reinvest any profit generated back into the entity in order to fulfil its purpose. All NFPs have a responsibility to remain solvent, generate sufficient profit for the long-term sustainability of the organisation through diverse funding streams (i.e. apart from membership contributions alone), and the judicious management of funds to benefit the ongoing viability of the organisation.

As noted above, there are important considerations for directors when seeking and obtaining funding from grants and donors that have specific objectives. Competition for funding can lead NFPs to move into the provision of services that are related to, but misaligned with, the NFP's overall mission and strategy. This is where a strong governance framework for managing risk and opportunity is critical – and it is the duty of the board to ensure that these frameworks are in place, and that member interests are being met through the achievement of the organisation's purpose.

STAKEHOLDER ENGAGEMENT

As highlighted in [Chapter 8 Stakeholder Engagement](#), all boards have an accountability to their stakeholders. An NFP director's individual role is to represent its members and communities. Part of this responsibility includes providing stakeholders with adequate channels for raising concerns and reporting back to stakeholders on a transparent and regular basis. In the discharge of their duties, an NFP director should recognise the diversity of the membership, be aware of the members' needs and balance the varying demands and incorporate these into the strategic priorities of the NFP entity.

As a collective, an NFP entity's board must also engage across the membership. This often facilitates the individual director and overall board's understanding of the different needs and challenges facing the members and informs their oversight role. Member engagement can take many forms, both informal and formal. It can include representation or participation in member forums, attendance at related events, visitation plans and liaising with membership groups.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Members have wide and varied expectations that the NFP entity will fulfil most/all relevant needs. Obtaining value for money and the cost of membership are often critical issues for members.

Outputs of the engagement process should inform strategy development and priority setting. This will keep the NFP's thinking fresh and ensure that member needs and the NFP's overall mission are being met.

Directors should also be aware of the importance of stakeholder engagement and the approach taken to engage stakeholders on decisions and strategy. Stakeholders can, in this instance, include relevant government departments, funders and sponsors, industrial bodies, education providers, research institutes and collaborators and community interest groups.

NFP entities should have a policy in place for communicating and engaging with stakeholders to ensure a consistent approach is taken across the NFP entity and that discussions with the relevant key and critical stakeholders (government departments) are not approached on an 'ad hoc' individual basis.

IDENTIFICATION, MANAGEMENT AND MITIGATION OF RISK

Risk management is a critical function for any organisation, particularly the board. NFP boards have some unique risks that require additional consideration, including ensuring the health and safety of staff and volunteers – who can often be placed in dangerous situations. For example, NFPs that provide health and support services to mental health patients, may have volunteers who assist in delivering these services. The volatile nature of members may place these volunteers at risk of injury or stress. To adequately fulfil their duties, directors need to ensure that they are cognisant of the unique circumstances and potential legal, reputational and physical risks that exist within their operations.

Resilience to long-term and emerging risks

Long term strategic initiatives with a focus on sustainable functionality, and the NFP entity's ability/agility to respond to varying external impacts/challenges, are critical for both corporate and NFP boards. However, the ability of an NFP entity to continue to deliver community services in the face of long-term social and environmental challenges needs to be understood and scenario-tested within the NFP entity's risk tolerance and risk appetite frameworks. For example, the World Economic Forum (WEF) lists issues such as ageing population, growing income disparity, natural resources shortages, increasing urbanisation, climate change and cyber disruption as key long-term global risks. NFP entities providing community services to support – for example – 'at risk' communities (e.g. elderly, disadvantaged), protection of the environment, provision of health services, etc. need to understand the potential risks and impacts on their ability to provide services. This includes identifying potential opportunities associated with these emerging risks, for example, new funding opportunities may eventuate in research and innovation around new areas of community need and support.

Chapter 18 *Environmental, Social and Governance (ESG)* provides more insight into the role of boards in managing sustainability risks and developing response strategies.

Similarly, it is critical that NFPs are aware of both the risks and opportunities generated by social media. The nature and volume of (mis)information spread through social media (and the speed at which this can occur) creates enormous reputational risk that can significantly impact any organisation's 'social licence to operate'. This is a particularly high risk for NFPs that are often in highly competitive funding environments. Conversely, the opportunities that social media can create for NFPs is also large and somewhat untapped. Awareness, support and even fundraising activities can be more quickly and effectively achieved through the reach and power of social media.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

As for all organisations, directors need to ensure that the NFP entity has in place a detailed risk management plan that is reviewed regularly. The board or subcommittee will often have responsibility for identifying risks and mitigation strategies, and endorsing actions when issues emerge.

Efficient and effective ability to monitor progress using agreed Key Performance Indicators (KPIs)

In many NFP entities, the expectation of transparent and timely disclosure of performance is critical to ensuring ongoing viability, by demonstrating progress towards ongoing positive contributions to member/constituent and public benefit.

Measuring progress against objectives via sound planning and governance processes is, therefore, critical for any NFP entity to maximise the opportunities for ongoing funding and support from stakeholders.

RECEIVING ASSURANCE

Assurance over NFP entities sits with different assurance and investigative bodies within the regulators that apply to the NFP entity.

Incorporated Associations in Australia are governed by each state and territory's Associations Incorporations Act. The auditing and reporting requirements are established by each local jurisdiction and, therefore, reference to the relevant legislation is required. For example, in Victoria, an annual audit is required, but only if revenue is greater than \$1,000,000. The auditor must be a registered company auditor, a member of CPA Australia or CA ANZ, or a person otherwise approved by the Registrar – Section 99 2(d) of the *Associations Incorporated Reform Act 2012*.

Useful resources

- AICD, The Not-for-Profit Governance Principles, <https://www.aicd.com.au/corporate-governance-sectors/not-for-profit/studies/2024-not-for-profit-governance-principles.html>
- Australian Charities and Not-for-Profit Commission <https://www.acnc.gov.au/>
- Pearce. R, 2020, Exit the federation? New governance structures emerging in NFP organisations, <https://thinkinsightadvice.com.au/new-governance-structures-nfp-organisations>

For further information please contact:



Stephen Isaac

**Partner, Audit
KPMG Australia
stephenisaac@kpmg.com.au**

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

5. Proprietary Limited Companies

Proprietary limited (proprietary) companies are the most common company type in Australia. This chapter outlines the key differences between proprietary companies and other company types.

In this chapter

- Key differences between public companies and proprietary companies
- Approaches to governance
- Financial statements requirements
- Crowd-sourced funding

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Has the company adopted a constitution or is it governed by the Corporations Act 'Replaceable Rules'?
2. Is there an overarching shareholders' agreement or trust deed (for those proprietary limited companies that act as trustee of a trust) to be considered in conjunction with the company constitution/ Replaceable Rules?
3. If the company predates the mid-1990s, has the board considered proposing the adoption of a new constitution to the company member(s)?
4. If the company is a wholly-owned subsidiary, does the company's constitution include the relevant clause to support this?
5. If the company is a family enterprise, does the company's share capital structure adequately facilitate the long-term succession of the company to the next generation?
6. If the company intends to avail itself of crowd-sourced funding, is it correctly structured to do so?
7. If the company is part of a larger group structure, is an up-to-date group structure chart maintained and readily available/accessible?
8. Has the company adequately maintained its financial records, minute book and statutory registers?
9. Has the company adequately documented and implemented a tax governance framework?
10. Is the company required to prepare, audit and/or lodge annual financial statements?
11. If the company is availing itself of ASIC relief from the requirement to prepare, audit and/or lodge annual financial statements, does the company adhere to the ongoing relief requirements?
12. If the company is required to lodge financial statements with ASIC or has constituent documents dated after 1 July 2021, have directors considered the new General Purpose Financial Statement reporting requirements?

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The board has not given adequate consideration to (or review of) the insurance of the company and its officers against possible liabilities.
- The family enterprise has not given due consideration to the governance of the family versus the governance of the business.
- Multiple subsidiaries exist in the group, but there is no up-to-date group structure readily available (and it is unclear who is responsible for maintaining it).
- Financial records and/or inter-group transactions are not properly documented.
- An ASIC directorship search reveals multiple out-of-date and/or inconsistent details for a director.
- The company's memorandum and articles of association predate the mid-1990s and no consideration has been given to their review and/or adoption of a new constitution.
- The directors are unaware of (and/or do not refer to) the existence of an overarching shareholders' agreement or trust deed.
- The company is not adequately structured for the long-term strategic goals or succession planning of the enterprise.
- If the company is availing itself of ASIC relief from the requirement to prepare, audit and/or lodge annual financial statements, the directors do not ensure that the company continues to satisfy the ongoing relief requirements.
- The board has not reconsidered its financial reporting requirements since 1 July 2021.
- No tax governance framework is documented or implemented.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

KEY DIFFERENCES BETWEEN PUBLIC COMPANIES AND PROPRIETARY COMPANIES

The majority of registered companies in Australia are proprietary limited companies. Like public companies, proprietary companies offer a limited liability to its members. However, there are a number of key differences between public and proprietary limited companies, including:

- Proprietary companies are limited by shares (or be an unlimited company with a share capital)¹ and are 'for profit' in nature (i.e. they cannot be used for not-for-profit purposes, unlike public companies that can be limited by guarantee and registered as not-for-profit organisations with the ACNC).
- They are not permitted to offer/sell shares directly to the public that would require disclosure under Chapter 6D of the Corporations Act.
- They are limited to a maximum of 50 (non-employee) shareholders.
- They are not able to list on the ASX and, therefore, are not subject to the ASX Listing Rules.
- Directors may be permitted to vote on matters where there is a personal material interest being considered at a directors' meeting.²
- They are subject to reduced requirements under the Corporations Act, including:
 - no requirement to have more than one director
 - facility for a sole director and member company³
 - no requirement to appoint a company secretary
 - no requirement to hold an AGM
 - possible exemption from preparing, auditing and lodging financial statements with ASIC.

¹ Corporations Act 2001, Section 45A(1) Note 2; Section 112(1).

² Corporations Act 2001, Section 194.

³ Corporations Act 2001, Section 198E.

The majority of these reforms were made to the corporations legislation. Therefore, companies whose Memorandum and Articles of Association (M&As) refer to pre-1990s corporate legislation and, as a consequence, may not be able to avail of these reduced requirements. In such instances, the company's M&As may need to be amended or repealed and replaced by the adoption of a modern constitution document.

It is important to note that the reduced requirements under the Corporations Act do not lessen the company and directors' exposure under other legislation, e.g. Work Health & Safety legislation. Directors must familiarise themselves with the responsibilities arising from other legislation and regulations, and should consider insuring against liabilities, where possible and appropriate.

APPROACHES TO GOVERNANCE

The governance of a proprietary company can vary immensely depending on its structure and purpose. Regardless of the simplicity of the company structure, all directors are still subject to their fiduciary duties, including but not limited to:

- the duty to act in good faith and exercise power for a proper purpose
- the duty to exercise skill and care.

They are also subject to other statutory duties, including the duty not to trade while insolvent.

Director remuneration

In respect to directors' remuneration, the constitution should set out the mechanisms for the approval and reporting of directors' remuneration. If the Replaceable Rules, Section 202A(1) or 202C of the Corporations Act have been followed, the total amount to be paid to directors should be approved by the company by resolution. Constitutions may contain more specificity concerning the approval and reporting mechanisms.⁴

⁴ Refer to AICD Directors' fees, 2020, <https://www.aicd.com.au/board-of-directors/career/salary/directors-fees.html>

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Sole director/member

A sole director/member company is the simplest of company structures. The Corporations Act includes a number of clauses that relate specifically to these companies. For example, Section 201F of the Corporations Act sets out the governance provisions for the circumstances that arise in the death or incapacity of the sole member/director.⁵

Trustee companies

It is common for trusts to appoint a corporate trustee, rather than individual trustees. This applies to private family trusts, unit trusts and self-managed superannuation funds. The management of the trustee company's affairs will typically parallel those of the underlying trust, however, the assets of the entity will lie in the trust rather than the company.

Section 19 of the *Superannuation Industry (Supervision) Act 1993* requires superannuation fund trustee companies to adopt a constitution that specifically notes that the company's sole or primary purpose is to act as trustee of the fund. The trustee company's constitution must also prohibit the company from distributing income or property to its members.⁶ Importantly, all directors of a self-managed superannuation fund (SMSF) trustee company must also be trustee company shareholders and all trustee company shareholders must be trustee company directors too for an SMSF to be compliant under Australian Income Tax Law.

Director identification number⁷ requirements apply equally to directors of trustee companies as they do to directors of operating companies. These are discussed further in [Chapter 9](#).

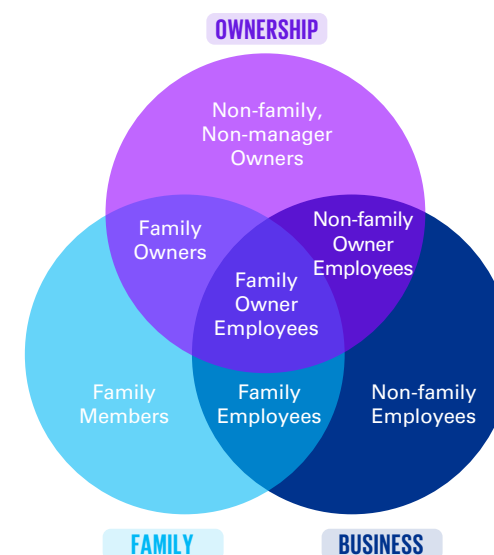
⁵ Corporations Act 2001, Section 201F.

⁶ Refer to ASIC, Special Purpose Companies, <https://asic.gov.au/for-business/registering-a-company/steps-to-register-a-company/special-purpose-companies/>

⁷ Refer to ABRS, Director Identification Number, <https://www.abrs.gov.au/director-identification-number>

Family enterprises

Family enterprises can often take the form of a proprietary company. The governance of the family can be challenging due to three interdependent and overlapping stakeholder groups being family, ownership and business. Good practice seeks to implement a framework that recognises that long-term success depends upon healthy functioning governance across all three key groups. Clarity and alignment within the family business system, depicted in the diagram below, enables the family to work cohesively towards its collective aspirations, and balance the needs and goals of individuals with the needs and goals of the collective family, the owners and the family business.

Three-circle model of the family business system⁸

⁸ Renato Tagiuri and John A Davis, 1996, Family Business Review, Bivalent Attributes of the Family Firm, refer to <https://journals.sagepub.com/doi/abs/10.1111/j.1741-6248.1996.00199.x>

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

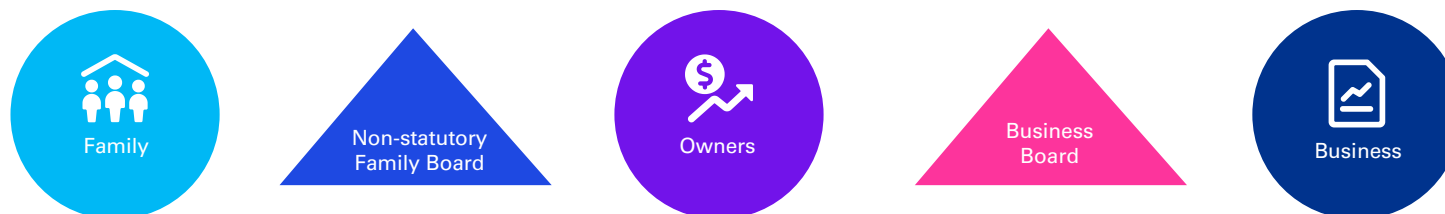
18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

It is important to clearly differentiate between the roles of owners, those in the business and other stakeholders in a family system. A family charter is often complemented by a shareholders' agreement and/or a family constitution document governed by a possible Family Council or Advisory Board. These additional layers of governance support the long-term strategy and succession planning for the family enterprise.



Underpinned by...				
– Binding Financial Arrangements – Trusts – Wills – Family Council	– Family Constitution • Statement of principles and rules, not binding • Pre-agreed rules • Family Charter, values	– Shareholders Agreement • Directorships • Buy/sell mechanisms • Delegated authorities • Rights of owners • Succession plan	– Board Charter • Skills matrix • Roles & responsibilities • KPIs • Delegated authorities	– Roles & job descriptions for family and non-family members – Authority & accountabilities – Goals – Performance development & management of family and non-family members

Pitfalls of nepotism, inequality and blurred boundaries commonly arise as the family enterprise matures, and can become more pronounced at times when the family enterprise is going through a significant change, such as a transition to the next generation. It is important that advisers to the family enterprise recognise these pitfalls are not uncommon and work with the family and the family enterprise to educate and guide decision-making.

Wholly-owned subsidiaries

Wholly-owned subsidiaries differ in nature by virtue of being owned and controlled by a parent company. The parent company can be another Australian company or a foreign-registered company.

Directors of large groups should ensure that an up-to-date group structure is maintained and readily available, and assign responsibility for it to an appropriate director or member of management.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The Corporations Act specifically allows a company's constitution to include a provision to assist with subsidiary director duties.⁹ Section 187 of the Corporations Act provides that the directors of a wholly-owned subsidiary can be taken to be acting in good faith in the best interests of the subsidiary if:

- the constitution of the subsidiary company expressly authorises
- the director to act in the best interests of the parent company the director acts in good faith in the best interests of the parent company
- the subsidiary is not insolvent at the time of the director's acts and does not become insolvent because of the director's acts.

Details of delegated authorities are usually captured in the corporate group's delegations policy. However, a group's delegations of authority may not provide clarity on whether the directors of a subsidiary company have a right to approve major transactions. In such cases, directors should seek clarification from the owner of the group delegations policy. A failure to consider important transactions undertaken by the subsidiary company could potentially place directors in breach of their duty to exercise skill and care.¹⁰ Directors should also take care that loan agreements and debt forgiveness between group entities is also adequately documented.

Directors who are appointed to multiple companies' boards should ensure that any changes to their personal details are notified to ASIC (and other relevant regulators and authorities) in a timely manner, for all affected entities. The periodic purchase and review of an ASIC directorship search is a useful exercise in this regard.

⁹ Corporations Act 2001, Section 187.

¹⁰ Refer to the Governance Institute of Australia, Guidelines for directors of wholly-owned subsidiary companies (membership required to access resources), <https://www.governanceinstitute.com.au/>

FINANCIAL STATEMENTS REQUIREMENTS

Section 286 of the Corporations Act requires all companies' financial records to be kept for at least seven years after the transactions covered by the records are complete. They must correctly record and explain the company's transactions, financial position and performance, and allow true and fair financial statements to be prepared. This obligation exists regardless of whether the company's books and records are maintained in-house or outsourced to a third party, and whether they are electronic or not.¹¹ Even if the company's records are held by someone else (e.g. an accountant), the directors, as company officeholders, are still responsible for providing copies to auditors or anyone entitled to inspect the records.¹²

Section 292 of the Corporations Act outlines which companies must prepare annual financial reports and directors' reports. A 'large' proprietary company must prepare and lodge with ASIC a financial report, a directors' report and an auditor's report¹³ within four months after the end of the company's financial year.¹⁴ The financial report, directors' report and auditor's report must also be given to members within these four months.¹⁵

¹¹ Refer to ASIC, Directors and Financial Reporting, <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/directors-and-financial-reporting/>

¹² Refer to ASIC, What books and records should my company keep?, <https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/what-books-and-records-should-my-company-keep/>

¹³ Corporations Act 2001, Section 301(1).

¹⁴ Corporations Act 2001, Section 319(3)(b).

¹⁵ Corporations Act 2001, Section 315(4).

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Definition of 'large' company or group

A proprietary company is 'large' if it meets at least two of three thresholds listed in the below table at the end of a financial year. The current thresholds replaced those from 2007 on 1 July 2019.

	Threshold
Consolidated revenue for the financial year of the company and the entities it controls*	\$50 million
Value of the consolidated gross assets at the end of the financial year of the company and the entities it controls*	\$25 million
Employees^ of the company and the entities it controls	100 employees

* Control is determined based on whether accounting standards require the company to prepare financial statements in relation to a consolidated entity.

^ Part-time employees are counted as an appropriate fraction of the full-time equivalent.

A 'small' proprietary company is only required to prepare, audit and lodge financial statements with ASIC if it is controlled by a foreign registered company (and its financial information is not consolidated into the financial statements of the foreign registered company, registered scheme or disclosing entity) or if the company is directed to do so by ASIC, or by 5 percent or more of their shareholders.¹⁶

Financial reporting obligations for certain proprietary companies significantly changed from 1 July 2021 with the introduction of AASB 2020-2 'Removal of Special Purpose Financial Reports for Certain For Profit Private Sector Entities'. Where proprietary companies are required under legislation to prepare financial statements in accordance with Australian Accounting Standards or 'accounting standards', or their constitutions or other key governance documents (such as bank lending agreements), commencing or amended on or after 1 July 2021, require preparation of financial statements in accordance with Australian Accounting Standards, these companies will be required to prepare Tier 2 General Purpose Financial Statements (GPFS).

Where directors of proprietary companies have relied on preparing special purpose financial statements (SPFS) in the past, it is recommended that directors and advisers revisit the reporting/non-reporting entity classification and ensure that their reasoning for continuing SPFS is comprehensively documented or whether indeed GPFS are now required.

ASIC relief relating to financial statements

In certain circumstances it is possible for proprietary companies to avail themselves of exemptions from the requirements to prepare, audit and/or lodge financial statements with ASIC. ASIC relief instruments include:

- ASIC Corporations (Foreign-Controlled Company Reports) Instrument 2017/204 (formerly ASIC Class Order 98/98)¹⁷
- ASIC Corporations (Wholly-owned Companies) Instrument 2016/785 (formerly ASIC Class Order 98/1418)¹⁸
- ASIC Corporations (Audit Relief) Instrument 2016/784 (formerly ASIC Class Order 98/1417).¹⁹

¹⁷ ASIC Corporations (Foreign-Controlled Company Reports) Instrument 2017/204 available at <https://www.legislation.gov.au/Details/F2017L00307>

¹⁸ ASIC Corporations (Wholly-owned Companies) Instrument 2016/785 available at <https://www.legislation.gov.au/Details/F2016C01085>

¹⁹ ASIC Corporations (Audit Relief) Instrument 2016/784 available at <https://www.legislation.gov.au/Details/F2016L01542>

¹⁶ Corporations Act 2001, Section 292.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The ASIC website,²⁰ ASIC Regulatory Guide 58 'Reporting by registered foreign companies and Australian companies with foreign shareholders'²¹ and ASIC Regulatory Guide 115 'Audit relief for proprietary companies'²² provide further guidance in relation to the requirements for proprietary companies wishing to avail themselves of the relief.

It is important to note that ASIC relief instruments do not exonerate any company from the requirement to prepare or audit financial reports if directed to do so by ASIC²³ or its shareholders.²⁴ Nor does the relief exempt the company from the requirement to retain financial records.²⁵

If the board resolves that the company is eligible to avail itself of relief under a specific ASIC Instrument, it should review the relevant ASIC Instrument at least annually and ensure that the company continues to comply with the ongoing Instrument requirements.

GOVERNANCE AND INCOME TAX

Directors and advisers should be aware of the ATO's Private Group review programs and be cognisant of the issues that are likely to attract attention. Private groups are becoming a greater focus for the ATO, as they are often confronted by the same issues as larger businesses and corporations, however, face a host of other issues arising from the private nature of their business and ownership. These issues include the complexities of family dealings and the consequences of employing different ownership structures.

²⁰ Refer to ASIC, Lodgement of financial report (INFO 31), <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/preparers-of-financial-reports/lodgement-of-financial-reports/>

²¹ Refer to ASIC, Regulatory Guide 58, June 2020, Reporting by registered foreign companies and Australian companies with foreign shareholders, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-58-reporting-by-registered-foreign-companies-and-australian-companies-with-foreign-shareholders/>

²² Refer to ASIC, Regulatory Guide 115, June 2020, Audit relief for proprietary companies, <https://download.asic.gov.au/media/5689855/rg115-published-19-june-2020-20200727.pdf>

²³ Corporations Act 2001, Section 294.

²⁴ Corporations Act 2001, Section 293.

²⁵ Corporations Act 2001, Section 286.

The ATO is now devoting significant resources to assuring the taxation and superannuation obligations of private groups. Critical to achieving a 'justified trust' rating with the ATO is having a robust tax governance framework in place. Directors should ensure they have clear processes and procedures within a corporate governance framework to support the proprietary company's tax decision-making and manage tax and super risks.

Proprietary company directors, like their public company counterparts, are individually personally liable to pay any outstanding liability where a company that they are a director for fails to meet obligations pertaining to pay as you go tax (PAYG), the superannuation guarantee charge and the goods and services tax (GST).

CROWD-SOURCED FUNDING

Crowd-sourced funding (CSF) is a financial service where startups and small businesses raise funds, generally from a large number of investors that invest small amounts of money. A provider of CSF services must hold an Australian Financial Services (AFS) licence.

The *Corporations Amendment (Crowd-sourced Funding for Proprietary Companies) Act 2018* took effect from 19 October 2018 and makes further changes to the law to extend the CSF regime to eligible proprietary companies. Under the CSF regime, eligible proprietary companies will be able to make offers of their shares, via an intermediary CSF service, using an offer document.²⁶

The Act includes requirements for proprietary companies wishing to use the CSF regime, including that the company must:

- maintain a minimum of two directors
- have their financial reports audited once they raise \$3 million or more from CSF offers
- comply with the existing related party transaction rules that apply to public companies.²⁷

²⁶ Refer to ASIC, Crowd-sourced funding, <https://asic.gov.au/regulatory-resources/financial-services/crowd-sourced-funding/>

²⁷ *ibid.*

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

There are obligations and investor protections that apply to CSF offers, including:

- an investor cap of \$10,000 per annum per company for retail investors
- the provision of a CSF offer document containing minimum information and a prescribed risk warning
- a five-day cooling-off period.²⁸

ASIC's Regulatory Guide 261 'Crowd-sourced funding: Guide for companies' is a guide for companies seeking to raise funds through CSF.²⁹

Useful resources

- ASIC information sheet (INFO 183) 'Guide Directors and financial reporting' available at [https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/directors-and-financial-reporting/ASIC-information-sheet-\(INFO-76\)-What-books-and-records-should-my-company-keep/](https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/directors-and-financial-reporting/ASIC-information-sheet-(INFO-76)-What-books-and-records-should-my-company-keep/) available at <https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/what-books-and-records-should-my-company-keep/>
- ASIC information sheet (INFO 79) 'Your company and the law' available at <https://asic.gov.au/for-business/running-a-company/company-officeholder-duties/your-company-and-the-law/>
- Governance Institute of Australia's 'Difference between private and public company structure under the Corporations Act' chart available on its website (for members only) www.governanceinstitute.com.au Corporations Amendment (Proprietary Company Thresholds) Regulations 2019 available at <https://www.legislation.gov.au/Details/F2019L00538>
- Key facts: AASB 2020-2 Amendments to Australian Accounting Standards – Removal of Special Purpose Financial Statements for Certain For-Profit Private Sector Entities, https://www.aasb.gov.au/admin/file/content102/c3/AASB2020-2_KeyFacts_03-20.pdf

²⁸ *ibid.*

²⁹ Refer to ASIC, Regulatory Guide 261, June 2020, Crowd-sourced funding: Guide for companies, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-261-crowd-sourced-funding-guide-for-companies/>

- ATO's Tax governance guide for privately owned groups, <https://www.ato.gov.au/Business/Private-owned-and-wealthy-groups/Tax-governance/Tax-governance-guide-for-privately-owned-groups/> Bivalent Attributes of the Family Firm, Renato Tagiuri and John A Davis, 1 June 1996

For further information please contact:



Robyn Langsford
Partner,
Family Business & Private
KPMG Australia
rlangsford@kpmg.com.au

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

6. Indigenous Culture

Australian businesses operate on land that is rich with history. Boards have an important role to play in creating policies and culture which not only advance reconciliation and pay respect to First Nations people, but also increase economic equity.

In this chapter

- Understanding First Nations culture to strengthen governance and performance
- The role of the board in advancing reconciliation and economic equity
- Governance considerations for Indigenous organisations

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that directors should ask

1. Does the organisation have a Reconciliation Action Plan?
2. How does the organisation recognise and celebrate the traditions and culture of the First Nations people of the countries where we operate?
3. Is the board equipped to engage confidently with First Nations' stakeholders?
4. Do directors, executives and staff demonstrate cultural competency?
5. What programs are in place to promote procurement and partnering with Indigenous corporations?
6. Are goals to increase First Nations representation across the workforce being achieved?
7. Has the board considered how governance may need to evolve to better support objectives pertaining to diversity and inclusion with regard to First Nations people?
8. How well do we understand the governance practices and customs of our Indigenous partners and how are we working towards ensuring mutual benefits?

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The organisation does not have, or intend to have, a Reconciliation Action Plan.
- There is an inability to attract or retain First Nations staff, customers and suppliers.
- Acknowledgements of Country are seldom made and/or are not respectfully delivered.
- Directors display a lack of appreciation for the cultural values of First Nations people.
- The importance of respecting First Nations heritage is not communicated or actively demonstrated by the board or the executive.
- No partnerships or contracts have been established with any Indigenous organisations.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

UNDERSTANDING FIRST NATIONS CULTURE TO STRENGTHEN GOVERNANCE

The focus of this chapter is twofold.

1. Support directors in incorporating policies and practices which embrace the full richness of Australia's culture and support reconciliation in the organisation.
2. Highlight how governance in Indigenous organisations may be different in certain aspects. There is much to learn from those that came before, especially as the world increases focuses on ESG. Whilst most of the corporate governance frameworks in OECD countries have only relatively recently incorporated aspects of culture, it is observed through the Indigenous Governance Toolkit (described as 'an online resource developed for Indigenous nations, communities, individuals and organisations searching for information to build their governance')¹ that Indigenous governance has culture in the centre of how governance is approached.

THE ROLE OF THE BOARD IN ADVANCING RECONCILIATION AND ECONOMIC EQUITY

The board sets the tone for the organisation through policies created ('what it does') but also through words and actions ('what it says'). Accordingly, the board should be examining how policies (and related key performance indicators) can be adapted to drive necessary change which embraces the culture and heritage of all people connected to where the organisation operates and has an impact. For some organisations this may require a cultural change program to fast-track the change required, especially where the organisation wants to be a leader in this area. At a minimum, whole-of-organisation cultural awareness training to support policies being implemented is considered better practice in building common understanding and appreciation.

¹ Refer to Indigenous Governance Toolkit at <https://toolkit.aigi.com.au/>



Case study: Microsoft Australia

Microsoft Australia's Managing Director, Steven Worrall, identified that his staff across Australia would benefit from Arrilla (a majority Indigenous-owned organisation in which KPMG has invested) providing training on how to confidently engage with Indigenous suppliers, stakeholders and businesses. Steven Worrall describes the benefits derived from this training in a video on the KPMG website² and, in summary, he states that the training fostered an understanding of Indigenous culture, a sensitivity to diversity, and a greater sense of inclusiveness, as well as decreasing unconscious bias.

Commercially, by breaking down stereotypes about Aboriginal and Torres Strait Islander people and businesses, Microsoft Australia's staff were enabled to more readily engage with Indigenous companies and suppliers. The flow-on benefits of this increased economic engagement (e.g. including increased economic activity of Indigenous businesses), will continue to generate positive results across the communities Microsoft works with.

² KPMG, Microsoft Australia: driving Indigenous culture competency in the workplace, <https://home.kpmg/au/en/home/insights/2019/01/microsoft-australia-indigenous-cultural-competency-workplace-client-story.html>

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

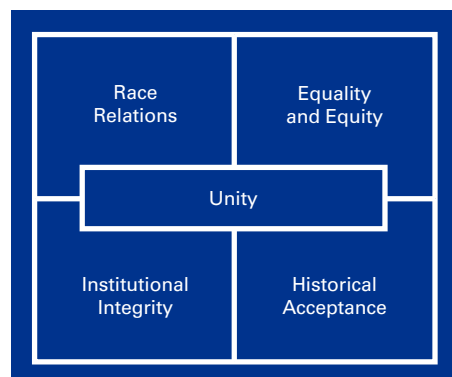
CONTACT US

As with any cultural change, unless the board actively engages and is seen to be changing how it operates, positive sustainable change is unlikely to occur. Ian Hamm (a Yorta Yorta man from Shepparton in central Victoria) spoke at the AICD's 2021 Australian Governance Summit encouraging more diversity in the boardroom to provide a 'better understanding of the social contract' that organisations are part of.

Reconciliation

Supporting reconciliation is one way that leading organisations are delivering on the aforementioned social contract. Reconciliation Australia describe reconciliation as being 'about strengthening relationships between Aboriginal and Torres Strait Islander peoples and non-Indigenous peoples, for the benefit of all Australians'.³

Reconciliation Australia describe that reconciliation is based (and measured) on the five dimensions shown in the diagram below:



Source: Reconciliation Australia⁴

To bring reconciliation to life within organisations, at the time of writing this, over 3,200 organisations have developed Reconciliation Action Plans (RAPs) to embed the principles and purpose of reconciliation, reflecting a significant increase in the number of organisations seeking to take meaningful actions to advance reconciliation. Connected to ESG objectives, most organisations with RAPs proudly promote this fact, building awareness of the reconciliation imperative whilst also potentially benefiting from the incidental commercial benefit.

Making a decision to pursue a RAP is an investment and the implementation of actions needed may see policies and even potentially strategic objectives needing to be adapted. Accordingly, it would be expected that the decision to develop a RAP would be a matter reserved for the board to decide upon.

³ Refer to Reconciliation Australia at <https://www.reconciliation.org.au/reconciliation/>

⁴ *ibid.*

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ACKNOWLEDGEMENT OF COUNTRY

Acknowledgement of Country stems from the traditions of Australia's First Nations people who historically would seek permission before entering another's Country. Those to whom the Country belonged would in turn welcome the visitor to their Country. In the same way as the visitor would respect any customs and traditions of the Country being visited, and give thanks for being allowed to visit, it is considered good practice to include acknowledgment and heartfelt appreciation for a Country and its people at the start of any meeting or event.

Note that only Traditional Owners, or Aboriginal and Torres Strait Islander peoples who have been given permission from Traditional Owners to welcome visitors to their Country can deliver a Welcome to Country.

Reconciliation Australia recommend that the local Aboriginal Land Council or Native Title representative body can advise on organising a Welcome to Country by a Traditional Owner in the area where a gathering is occurring.

Directors should set the example for demonstrating their recognition of the heritage of the land that they are meeting on by consistently ensuring that a meaningful acknowledgement is included at the commencement of all gatherings and that this does not feel like an empty box-ticking exercise. Some organisations provide standard wording to be used in acknowledgements of Country which is one way to ensure a consistent message is delivered. Reconciliation Australia recommend the wording used could include something like the following:

'I'd like to begin by acknowledging the Traditional Owners of the land on which we meet today. I would also like to pay my respects to Elders past and present.'

or

'I'd like to begin by acknowledging the Traditional Owners of the land on which we meet today, the (people) of the (nation) and pay my respects to Elders past and present.'⁵

To identify the Traditional Owners of the land that the meeting is occurring on, the map of Indigenous Australia provided by AIATSIS can be consulted.⁶

One way to make the delivery meaningful is to bring any learnings gleaned about the Country and its people into the acknowledgement. This has the added benefit of also educating the audience thereby furthering understanding of culture and heritage.

5 Refer to Reconciliation Australia at <https://www.reconciliation.org.au/acknowledgement-of-country-and-welcome-to-country/#:~:text=An%20Acknowledgement%20of%20Country%20is,Strait%20Islander%20peoples%20to%20Country.&text=Aboriginal%20and%20Torres%20Strait%20Islander%20peoples%20may%20also%20wish%20to,other%20First%20Nations%20peoples%20present.>

6 Refer to AIATSIS, Map of Indigenous Australia, <https://aiatsis.gov.au/explore/map-indigenous-australia>

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ENGAGING MEANINGFULLY WITH FIRST NATIONS COMMUNITIES

A RAP is a helpful and tangible way for organisations to actively consider how they engage with First Nations communities, people and culture – either as employees, customers or suppliers.

Aboriginal and Torres Strait Islander people consider culture fundamental to governance. Their cultural values, traditions, rules and beliefs, although they may differ between communities and groups, continue to be fundamental to how they govern themselves. Consideration as to how to embed Indigenous cultural values should be at the forefront of developing and adapting an organisation's governance.

Engaging meaningfully means that organisations need to understand the context of First Nations' organisations, how they are governed, how they operate, their culture and priorities.

GOVERNANCE CONSIDERATIONS FOR INDIGENOUS ORGANISATIONS

It is important to recognise an organisation's governance history and determine how Indigenous governance will be incorporated into its future governance practices. As mentioned before, Aboriginal and Torres Strait Islander people consider culture fundamental to governance. Their cultural values, traditions, rules and beliefs, although they may differ between communities and groups, continue to be fundamental to how they govern themselves. Consideration as to how to embed Indigenous cultural values should be at the forefront of developing and adapting an organisation's governance.

CATSI Act and ORIC

Indigenous groups may benefit from becoming a corporation and a separate legal entity. These groups are able to be incorporated under a Commonwealth, state or territory law depending on the individual circumstances. The Corporations (Aboriginal and Torres Strait Islander) Act 2006 (CATSI Act) allows the Office of the Registrar of Indigenous Corporations (ORIC) to provide regulatory assistance and education. ASIC has set out the key differences between the CATSI Act and the Corporations Act covering members; directors; shares/debentures; types of corporations; financial services limitations; internal governance rules; regulatory assistance; registration requirements; reporting; merits review process; native title and fees,⁷ the key ones impacting directors are:



⁷ Refer to ASIC, The CATSI Act and the Corporations Act – some differences, <https://download.asic.gov.au/media/4907483/fact-sheet-catsi-act-vs-corp-act.pdf>

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

	Corporations Act	CATSI Act
Directors	– Any person can be a director; they don't need to be a member. – A proprietary (private) company must have at least one director, but doesn't need to have a secretary. The director and secretary (if there is one), must usually live in Australia. – A public company must have at least three directors and at least one secretary. At least two of the directors and one secretary must usually live in Australia.	– Corporations can have a rule in their rule book that allows people who are not members to be directors. However, the majority of directors must: • be Aboriginal or Torres Strait Islander • be members of the corporation • not be employees of the corporation. – The minimum number of directors is 3 and the maximum number is 12. Corporations can apply to the Registrar for an exemption if they want more than 12 directors. – The majority of directors must usually reside in Australia. – Large corporations must have a secretary. Small and medium corporations have a contact person.
Internal governance rules	A company can follow the replaceable rules in the Corporations Act or adopt their own constitution.	An Aboriginal and Torres Strait Islander corporation must have a rule book which, at a minimum, contains: – the objectives and name of the corporation – frequency of directors' meetings – a dispute resolution process. The corporation may adopt the replaceable rules in the CATSI Act or modify or replace them.

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Cultural-based governance principles

The Indigenous Governance Toolkit describes Indigenous governance as 'a networked form of governance. It is based on thick pathways and layers of relationships and connections between people, places and things, past, present and future.'⁸ Based on this, Indigenous people frequently apply the cultural-based principles in the diagram below to design their governance frameworks.



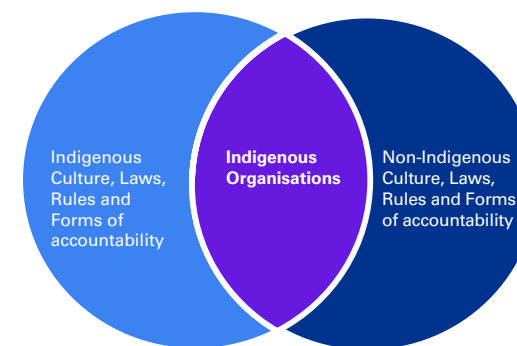
Indigenous Governance Principles in Australia (Source: Indigenous Governance Toolkit)⁹

As decisions are made on the organisation's governance structure, the board and management should consider the Indigenous traditions and values which are important to them and use these principles to reflect priorities.

⁸ Refer to Indigenous Governance Toolkit, <https://toolkit.aigi.com.au/toolkit/2-1-indigenous-governance-and-culture>

⁹ *ibid.*

As the diagram below illustrates, the Indigenous Governance Toolkit recognises that Indigenous organisations are required to find a way for the governance framework to integrate both internal requirements (the rules that govern their networks and communities) and external requirements (the rules that govern the external stakeholders which support their community or organisation).



The Two-Way Accountability of Indigenous Organisations And Governing Bodies (Source: Indigenous Governance Toolkit)¹⁰

This is achieved by creating governance structures which are innovative and robust to cater for the two systems of governance. Equally there are benefits for non-Indigenous organisations to consider how their frameworks may need to flex to work better with Indigenous organisations.

¹⁰ *ibid.*

FOREWORD

• THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- Reconciliation Australia, [Home – Reconciliation Australia](#)
- TED Talk on delivering an Acknowledgement of Country that really means something, Shelley Reys AO, https://www.youtube.com/watch?v=zxo18_7BDt4
- Indigenous Governance Toolkit, <https://toolkit.aigi.com.au/> (1)
- Office of the Registrar of Indigenous Corporations, <https://www.oric.gov.au/> (2)

For further information please contact:



Glen Brennan

Lead Partner, Indigenous Services
KPMG Australia
glenbrennan@kpmg.com.au

Governance Accountability

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

7. Accountability to Shareholders

Listed public companies are often jointly owned by a relatively large number of separate shareholders, including both individual and institutional shareholders. Individual shareholders (and potential shareholders) have different investment objectives, which are based on varying degrees of financial and commercial understanding, literacy, competency and market intelligence.

In this chapter

- Protecting shareholders' rights
- The board's role
- Shareholders' responsibilities
- The directors' role in investor relations
- Institutional shareholders' role in governance
- Effective annual general meetings (AGMs)
- Statutory reporting
- Statutory reporting content
- Annual report
- Directors' report
- Directors' declaration
- Auditor's report
- Other disclosures in the annual report
- Concise version of annual reports
- Half-year reports
- Audit
- Audit committee
- Continuous disclosure
- Investor decision-making
- The board's role in business reporting

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Do the chair and directors play an active role in the investor relations program?
2. Are mechanisms in place to capture market intelligence and investor feedback? This may include social media as a dynamic new data source.
3. Is the chair always well prepared for questions from the floor at the Annual General Meeting (AGM)?
4. Are there sufficient skills and experience amongst audit committee members to effectively review statutory reporting obligations?
5. Does the board have a process to ensure that all statutory reporting obligations are met in a timely manner?
6. Is there a continuous disclosure policy approved by the board and linked to the spokesperson policy?
7. Does the board regularly review the effectiveness of its business reporting and communication in assisting investor decision-making?
8. Is the reporting and communication strategy/ investor relations strategy part of the annual strategy development program?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The board is not aware of the identity or views of major investors.
- Major marketplace concern regarding executive remuneration incentives.
- The AGM is a major public relations challenge.
- There is no social media policy, monitoring or escalation procedures for unfavourable events.
- The investor relations manager has no contact with the board.
- There is no strategy of how to handle private equity approaches.
- Institutional investors publicly voice concerns regarding some of the organisation's governance practices.
- The ASX expresses concern regarding the timeliness of the organisation's market disclosures.
- The organisation's business model is not clearly articulated in external communications.
- The linkage between financial and non-financial reporting is not evident in external communications.
- A significant protest vote against the company's remuneration report.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The notion of accountability to shareholders is at the core of any corporate governance framework. Shareholders are certainly becoming more active in asserting their rights and many boards are responding by trying to engage with their shareholders more effectively. Nevertheless boards must balance the equitable treatment of shareholders and the protection of their rights against the need to create sustainable shareholder value.

PROTECTING SHAREHOLDERS' RIGHTS

A basic principle of corporate governance is that it should protect shareholders' rights. These rights typically relate to, but are not limited to:

- Declaring dividends in the best interests of shareholders.
- Receiving information pursuant to the company's continuous disclosure obligations.
- Approving changes to the company's constitution, articles of association or similar governing documents.
- Nominating and appointing directors.
- Receiving continuous disclosure of material developments in the company's affairs.
- Calling a general meeting of shareholders, and/or proposing a resolution to be considered at a general meeting.
- Voting at the AGM.
- Obtaining an independent valuation of their securities.
- Inspecting the minute books for members' meetings.
- Suing the corporation for wrongful acts.

THE BOARD'S ROLE

Governance authorities suggest there are some key board roles in protecting shareholder rights:

- Maintaining a detailed understanding of shareholders' rights that are set out in the Corporations Act, the ASX Listing Rules and other relevant legislation, together with the company's constitution and board policies.

- Maintaining up-to-date knowledge of the company's nominee shareholders and, to the extent possible, their underlying beneficial shareholders.
- Ensuring shareholder communication is open and transparent.
- Ensuring debate on contentious issues is embraced and prepared for.
- Implementation of shareholder proposals approved by a majority of votes/proxies cast at a general meeting.

SHAREHOLDERS' RESPONSIBILITIES

Shareholders have different investment objectives: some invest for short-term gain, some for long-term value, and others for socially responsible reasons. Companies with an effective approach to investor relations will understand the objectives of different investor groups and key individual investors. Communication and active engagement with shareholders generate feedback on investor concerns. Certain shareholders, particularly some institutional shareholders, are becoming more assertive in protecting their own rights and are taking various measures to influence the companies in which they invest. These measures include:

- Communicating with the company openly and transparently.
- Adopting a clear, comprehensive and pragmatic view of what constitutes good corporate governance.
- Understanding and monitoring company performance and providing feedback to the company.
- Teaming with like-minded shareholders to exert a collective influence.
- Lobbying and targeted activism.
- Engaging with the company's board in times of crisis, or with regard to major transactions, such as takeovers, mergers and private equity approaches, and capital raisings.
- Adopting consistent positions, where appropriate, on particular issues and voting accordingly.
- Publishing governance guidelines.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US



Centro case study: ASIC v Healey [2011] FCA 717

The directors of Centro companies signed off on financial reports with material errors, classifying short-term liabilities as long-term liabilities. The Federal Court found that in approving the financial statements, the directors had failed to discharge their duties with due care and diligence under sections 180(1), 344 and 601FD of the Corporations Act. The Centro decision reaffirms that whilst directors are not expected to possess specialist financial or accounting expertise, or to be involved in the day-to-day management of the company, they are expected to have the necessary level of competence to read and understand financial statements. Directors must independently and critically examine the accuracy and content of financial reports in the context of their knowledge of the company's affairs and activities, and cannot abrogate their responsibilities by placing sole reliance on management or external advisers, no matter how competent they appear to be.

Another case that has reinforced the behaviour expected of directors is the James Hardie case of *ASIC v Hellicar*.



James Hardie case study: ASIC v Hellicar [2012] 247 CLR 345

The non-executive directors approved a misleading announcement on the ASX that stated the company had fully funded its liabilities that related to asbestos disease when, in actual fact, there was a funding shortfall. The High Court held that the directors of James Hardie had contravened their duties of care.

SHAREHOLDERS CONVENING MEETINGS

Section 249D of the *Corporations Act 2001* (Corporations Act) requires directors of a company to call and arrange to hold a general meeting at the request of members with at least 5 percent of the votes that may be cast at a general meeting. In addition, if members with at least 5 percent of the votes that may be cast at a general meeting call and arrange to hold a general meeting, then those members who called the meeting must pay the expenses in relation to calling and holding the meeting.¹



Woolworths case study: Woolworths Ltd v Getup Ltd [2012] FCA 726; 90 ACSR 670

210 members requested the directors of Woolworths call a general meeting in order to put forward a special resolution to change its constitution to prevent ownership of poker machines. Woolworths requested an injunction for the meeting be held at the AGM as the meeting would have led to the incurrence of an additional \$400,000 in expenses. The Court did not consider a deferral to lead to substantial injustice and allowed Woolworths to defer the requisitioned meeting until its next AGM.

Shareholder and political activists have used the calling of general meetings as a platform to help promote political and social responsibility, notwithstanding the proposed resolutions might have a very low prospect of success or do not seek to maximise shareholder returns.

¹ Corporations Act 2001, Section 249F.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Remuneration and the two-strikes rule as a vehicle for shareholder activism

There has been a substantial increase in shareholder voting against remuneration reports for ASX 300 companies with the last three years' results as follows:

- 2024 – 40 companies (13.3%)
- 2023 – 41 companies (13.7%)
- 2022 – 22 companies (7.3%)

These votes are made not only as a means of signalling dissatisfaction with remuneration amounts or structures, but also to indicate shareholder expectations of the company's financial performance, governance and compliance have not been met.

Under the Corporations Act, the directors of a company are to be paid the remuneration that the company determines by resolution.² However, for public companies, director remuneration does not require member approval if it is reasonable.³

Voting against a publicly listed company's remuneration report has been a relatively recent encroachment that was prompted when the two-strikes rule was brought about in 2011. Put simply, all directors can potentially face re-election without a resolution being held under Section 203D of the Corporations Act.⁴ Under the two-strikes rule, when more than 25 percent of shareholders vote against the remuneration report for two consecutive years at the AGM, a 'spill motion' will be put to the company to spill the positions of all directors. That is, all positions vacated and a vote cast on whether to reappoint the board within 90 days.⁵

² Corporations Act 2001, Section 202A(1) (replaceable rule).

³ Corporations Act 2001, Section 211.

⁴ Corporations Act 2001, Section 203D.

⁵ Note also the restrictions that apply under sections 200-200J of the Corporations Act to termination payments by companies incorporated in Australia (and their associates) to those who hold a managerial or executive office in the company or in a related body corporate.

The two-strikes rule functions as a vehicle for shareholders to express their disapproval of directors' remuneration via the introduction of a 'spill meeting'.⁶ More broadly, it is a mechanism that activist shareholders can draw upon to indicate general discontent with the board and its performance. As part of the aftermath of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, several Australian financial services firms received a 'first strike' against their remuneration report. Prior to this, the 50 percent vote against Commonwealth Bank's report in 2016 was the historical record for an ASX 100 company. However, this was surpassed by AMP in 2018 with a 61 percent vote against its remuneration report,⁷ Westpac with 64 percent⁸ and NAB with 88 percent.⁹ This activism garnered immediate action by many companies to overhaul their remuneration schemes and governance. See the Myer case study below.

⁶ Corporations Act, Sections 250U-250Y. Under that rule, if 25% of the votes cast at two consecutive AGMs oppose the adoption of the remuneration report, then at the second AGM, shareholders can require that the board stand for re-election at a further general meeting to be held within 90 days. Shareholders can exercise this power if 50% or more of votes cast at the second AGM are in favour of a 'spill'. The requirement to stand for re-election does not apply to the managing director or any director appointed since the remuneration report was approved by the board.

⁷ Alice Uribe, 'AMP shareholders deliver historic first strike against AMP', Australian Financial Review, 10 March 2018, <https://www.afr.com/business/banking-and-finance/amp-shareholders-deliver-historic-first-strike-against-amp-20180510-h0zvki>.

⁸ Stephen Chalmers and Michael Janda, 'Westpac shareholders hit bank with first strike against executive pay', ABC News, 12 December 2018, <https://www.abc.net.au/news/2018-12-12/westpac-shareholders-hit-bank-with-first-strike/10610882>

⁹ Stephen Bartholomeusz, 'Banker's pay: There can only be one winner in this battle', Sydney Morning Herald, 27 March 2019 <https://www.smh.com.au/business/banking-and-finance/banker-s-pay-there-can-only-be-one-winner-in-this-battle-20190327-p517zq.html>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US



Case study: Myer

In late 2021, the board of directors of Myer narrowly avoided a board spill as their largest shareholder, Solomon Lew, who had a 15.7 percent stake joined with other shareholders to vote against the company's remuneration report (37 percent against) for the second consecutive time resulting in a spill motion. However, the spill motion did not receive majority support, meaning that the board were saved from having to stand for re-election.

As reported in the Sydney Morning Herald,¹⁰ Mr Lew had increased his shareholding earlier in the year with the intention of using his shareholding to drive a restructure of the board.

Given that as at 30 June 2025 no board has been spilled through this mechanism, it is likely that shareholders are concerned about the impact that a spill would have on the organisation and ultimately the risk of share price volatility.¹¹

THE DIRECTORS' ROLE IN INVESTOR RELATIONS

The board's role in formal investor relations continues to evolve. Many non-executive directors are now seeking to become more active in their companies' investor relations programs.

The investor relations function continues to increase in strategic importance. Investor relations teams have increasingly become responsible for communications, not only with the investment community, but also with internal stakeholders such as the board of directors, management and employees, by becoming responsible for, or at least influencing, coherent company messaging.

¹⁰ Dominic Powell, Sydney Morning Herald, 4 November 2021

¹¹ MinterEllison, February 2021, Key trends to emerge from the 2020 AGM season, <https://www.minterellison.com/articles/key-trends-to-emerge-from-the-2020-agm-season>

Boards are exposed to a number of risks if their organisation has inadequate investor relations expertise; regulatory risk (continuous disclosure and class actions), poor/lack of communication of strategy and performance to investors, and expectation for information to be publicly available in liquid markets for accuracy of share price valuation. Large companies operate in multiple dynamic, volatile markets and jurisdictions, with diverse investors with different goals requiring different communication strategies. Additionally, the risk of misleading and deceptive information being publicised on social media heightens companies' obligations to meticulously inspect their sources of information and make proper corrections. Boards need to understand their shareholders and shareholder segments, communicate their strategy appropriately, its performance and ESG activities and ensure the strategy is aligned to the company's best interests (being the interests of their shareholders as a whole).

At a minimum, and in conjunction with the board chair's traditional investor relations responsibilities, the board should approve any policies that control investor relations engagement risks. The board should also provide input into, and approve, the investor relations strategy as well as regularly monitoring investor relations activities. This strategy typically addresses an organisation's approach, performance targets and accountabilities for:

- shareholder and key stakeholder analysis and engagement planning
- shareholder services (including share registry and transactional support)
- investor targeting initiatives
- shareholder and key stakeholder communications
- media and public relations initiatives (including brand and reputation management)
- market intelligence and feedback mechanisms.

The ASX has recently begun to focus more on producing investor relations tools for ASX listed companies.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

INSTITUTIONAL SHAREHOLDERS' ROLE IN GOVERNANCE

Several sets of best practice principles have been published, addressing the responsibilities of institutional investors. One such example includes the International Corporate Governance Network's (ICGN) *Statement of Principles on Institutional Investor Responsibilities*,¹² which sets out its view of the responsibilities of institutional investors in relation to their external role as shareholders and also in relation to internal governance. With respect to voting responsibilities, the ICGN suggests that institutional investors should:

- disclose an annual summary of their voting records, together with their full voting records in important cases
- seek to reach a clear decision, in favour or against, for each resolution on which they are expected to vote
- disclose details of any outsourcing of ownership responsibilities (including the names of agents to whom they have outsourced, together with a description of the nature and extent of outsourcing and how it is regularly monitored).

Asset Owner Stewardship Code

The Australian Council of Superannuation Investors (ACSI) released the Australian Asset Owner Stewardship Code on 17 May 2018.¹³ It is the first guidance developed specifically for Australian asset owners in their role as equity holders in Australian-listed companies. The Code was established to increase the transparency and accountability of asset owners (including superannuation funds, endowments and sovereign wealth funds) when exercising their ownership rights in order to uphold value creation in their investments and ultimately protect and boost long-term investment performance for their beneficiaries.

¹² International Corporate Governance Network (ICGN), *Statement of Principles for Institutional Investor Responsibilities*, September 2013

¹³ Australian Council of Superannuation Investors (ACSI), *Australian Asset Owner Stewardship Code* (2024). <https://acsi.org.au/wp-content/uploads/2024/08/Australian-Asset-Owners-Stewardship-Code-2024-final.pdf>

Signatories to the Code are required to disclose details of essential stewardship activities including: voting, engagement, policy advocacy and the selection, appointment and monitoring of external asset managers. The disclosure requirement holds asset owners responsible for active ownership that will take into account ESG risks and opportunities, drive direct and collaborative engagement with investees and demonstrate awareness commitment to macroeconomic and regulatory issues.

EFFECTIVE AGMS

AGMs are governed by the Corporations Act (Part 2G.2), the company's constitution and common law. In the case of meetings of listed companies, public companies must hold an AGM of shareholders.¹⁴

For many public companies the AGM is a major exercise in shareholder communication and investor relations. The AGM offers shareholders a unique opportunity to question the board, express their views on company performance and suggest changes to company governance and operations.

As well as a forum for communication and discussion, the business of the AGM primarily considers the financial report and auditor's report, together with resolutions to approve the directors' report, and an advisory resolution for adoption of the remuneration report,¹⁵ and may include consideration of the appointment and remuneration of the auditor and the election of directors.¹⁶ Where the business of the meeting relates to the election (or re-election) of directors, shareholders will expect those directors to address them at the meeting.

Recommendation 9.3 of the ASX Principles also recommends that an external auditor attend the AGM and is available to answer questions from security holders at the meeting.

¹⁴ Corporations Act, Section 250N.

¹⁵ Corporations Act, Section 250R(1) and (2).

¹⁶ Corporations Act, Section 250R.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The following are some key considerations for AGMs:

- A hostile AGM is rarely the result of spontaneous combustion. Boards in touch with shareholder concerns will anticipate and embrace debate on contentious issues.
- Boards and management should spend time trying to anticipate specific shareholder questions and develop appropriate responses. Speakers should be identified in advance to respond to specific issues.
- Difficult or contentious questions can sometimes be short-circuited by raising and answering them in the annual report, or in the formal chair's address to the meeting.
- Shareholders can be invited to submit questions prior to the AGM.
- Shareholders should be able to access a webcast of the meeting; this is generally done by ASX 50 companies.
- The chair should be thoroughly familiar with the AGM agenda and meeting procedures, and have developed an approach for dealing with difficult or hostile 'responses' from the floor of the meeting.
- The chair must allow a reasonable opportunity for members to ask questions about or make comments on the management of the company.¹⁷

Under certain circumstances, shareholders can also compel directors to call extraordinary general meetings of shareholders,¹⁸ or seek to have resolutions added to the meeting agenda.¹⁹

In response to a request from the Federal Government for advice on the role of the AGM, in September 2012, the Corporations and Markets Advisory Committee (CAMAC) released a discussion paper entitled 'The AGM and Shareholder Engagement'. Over 35 submissions were received in relation to this review and an updated version was released in December 2012.

The updated paper provides useful guidance on shareholder engagement (including the regulation of proxy advisers), the purpose and format of the annual report, and the function and format of the AGM.²⁰

COVID-19 disrupted businesses in many ways, but one such disruption was the ability to hold an AGM in an environment where people were not able to gather in large groups. Temporary measures introduced to overcome this obstacle were made permanent in February 2022 with the Corporations Amendment (Meetings and Documents) Bill 2021 passing through Parliament. In addition to enabling the use of technology to distribute and execute documents, this Bill allows for AGMs to be conducted physically and virtually (if permitted by the entity's constitution) as well as applying a hybrid approach of both physical and virtual.

An important factor in making use of technology for virtual or hybrid meetings is that all shareholders continue to have the equivalent opportunity to participate that they would experience were they attending the meeting physically. To this end, ASIC has provided guidance on how questions and voting should be handled (polls to be used rather than a show of hands), how to support investors in accessing the meeting virtually, and also what to do when technical problems arise.²¹

Given that questions will now be able to be asked in writing via technology platforms utilised for the meetings, it is a positive step forward for inclusion of a cohort of the investor population who previously may have remained unheard in such forums.

20 Corporations and Markets Advisory Committee, 'The AGM and Shareholder Engagement', September 2019, https://takeovers.gov.au/sites/takeovers.gov.au/files/2021-04/agm_and_shareholder_engagement_discussion_paper.pdf

21 Refer to ASIC, August 2021, ASIC guidelines for investor meetings using virtual technology, <https://asic.gov.au/about-asic/news-centre/news-items/asic-guidelines-for-investor-meetings-using-virtual-technology/>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

STATUTORY REPORTING

Shareholder and investor communication starts with statutory reporting. For ASX listed companies in Australia, statutory reporting is based on:

- The Corporations Act and Corporations Regulations.
- Australian Accounting Standards, including interpretations (based on International Financial Reporting Standards [IFRS® Standards] issued by the Australian Accounting Standards Board [AASB]).
- ASIC Legislative Instruments that apply to the organisation.
- ASX Listing Rules.
- ASX Corporate Governance Principles and Recommendations 4th Edition.

The key elements of the statutory reporting portfolio for listed companies include:

- A half-year report, a preliminary final report and an annual audited financial report and directors' report (including the remuneration report).²²
- An annual Corporate Governance Statement and accompanying Appendix 4G.²³
- Notices for AGM.²⁴
- Additional disclosure requirements involving takeovers and new share issues.

²² See Chapter 2M of the Corporations Act and Chapter 4 of the ASX Listing Rules as to the content requirements of the half-year, preliminary final and annual reports. ASX also requires quarterly reports in certain circumstances (for instance, for mining companies or where a company has been listed under the 'assets test' requirement that half or more its total tangible assets are cash or readily convertible to cash) – ASX Listing Rule 4.7B.

²³ ASX Listing Rule 4.7.3, 4.7.4 and 4.10.3.

²⁴ Including notices of meeting (Corporations Act, Section 249J-L) and notices of resolutions (Corporations Act, Section 249O).

Whilst it is common practice for the board to allocate the oversight of statutory reporting to its audit committee, or equivalent, it is unable to abrogate its ultimate responsibility for the accurate and thorough preparation and timely release of statutory reports. Consequently, all directors need to understand not only the content of the reports, but what reports are required and by which authorities.

ASIC guidance suggests if directors take on a role with special responsibilities, such as the chair of an audit committee or the role of an executive director, you must discharge the increased responsibilities expected of directors in such positions with appropriate care and diligence.²⁵

Boards need to exercise appropriate due diligence in matters of financial disclosure. False or misleading statements could leave directors personally liable under the Corporations Act, the ASIC Act and Australian Consumer Law.

Boards should also insist that effective systems are in place to ensure all formal shareholder and investor communications (including financial reports):

- result from a designated approvals process
- include all the information required by the relevant laws and standards
- adhere to statutory timing requirements
- follow the format prescribed by the relevant laws and standards
- produce information that is accurate and not false or misleading (including by way of omission).

Some companies may also have reporting requirements to overseas regulators. For example, the US Securities and Exchange Commission (SEC) requires foreign registrants to file a number of reports and documents, including the comprehensive Form 20-F Annual Report of a Foreign Private Issuer.

²⁵ Refer to ASIC, Information Sheet 183 (INFO 183), Directors and Financial Reporting, <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/directors-and-financial-reporting/>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Unless members specifically elect to receive a hard or electronic copy of the annual financial report, companies or schemes can provide the annual financial report (or concise report) to its members by making it readily accessible on a website and by directly notifying members in writing that it has done so.²⁶

ASX Corporate Governance Principles and Recommendations (4th Edition)

The changes in the 4th Edition of the ASX Corporate Governance Principles and Recommendations primarily focused on culture, values and trust.

Principle 8.2 specifically addresses disclosure of remuneration policies and practices for directors; both executive and non-executive, and other senior executives.

In addition, the modification of Recommendation 4.3 in this edition shifted from ensuring validation of the financial reports to allowing investors to be satisfied about the integrity of a wider-ranging suite of information that they may use for their investment decisions. The recommendation is thus that 'a listed entity should disclose its process to verify the integrity of any periodic corporate report it releases to the market that is not audited or reviewed by an external auditor.'²⁷ 'Periodic corporate report' is defined in the glossary as 'an entity's annual directors' report, annual and half yearly annual statements, quarterly activity report, quarterly cash flow report, integrated report, sustainability report, or similar periodic report prepared for the benefit of investors.'

STATUTORY REPORTING CONTENT

Detailed guidance on the contents of the financial statements and notes to the financial statements can be obtained from KPMG's Financial Reporting Centre.²⁸

²⁶ Corporations Act, Section 314(1AA).

²⁷ ASX Corporate Governance Council, ASX Corporate Governance Principles and Recommendations (2019), 4th Edition.

²⁸ Refer to KPMG, Financial Reporting Centre, <https://home.kpmg/au/en/home/insights/2021/03/financial-reporting-centre.html>

ANNUAL REPORT

Depending on the entity's structure and jurisdiction, there are varying reporting requirements that must be adhered to. Directors should be aware of the reporting requirements and obligations applicable to the jurisdiction in which they operate. For example, a publicly listed entity in Australia is required to adhere to the statutory reporting requirements outlined in the previous section and any other applicable legislation relating to the entity type. For this reason, the contents of an annual report should include, at a minimum:

- Full set of financial statements, as defined by AASB 101, including the statement of financial position, statement of profit and loss and other comprehensive income, statement of cash flows, statement of changes in equity and explanatory notes. For financial years commencing on or after 1 July 2023, the financial report of a public company (listed and unlisted) includes a consolidated entity disclosure statement containing information about the tax residency of all its subsidiaries.²⁹
- Directors' report (including the remuneration report).
- Directors' declaration.
- Auditor's report and independence declaration.
- Corporate governance statement. (Listed entities have the option of making disclosures on their website or within the annual report. If an entity includes its corporate governance statement on its website; it must lodge a copy of the statement with ASX to have a permanent record as its effective date each year [listing rule 4.7.4]. Also, the annual report must include the website address where the corporate governance statement can be located.)

Increasingly, however, companies are choosing to include additional material in their annual reports. Emerging areas of optional reporting include sustainability, diversity, corporate citizenship and global taxation summaries,³⁰ which are being used to not only satisfy stakeholder demands for extra information, but also as a proactive step in the stakeholder management process.

²⁹ Corporations Act, Section 295(1)(b) and 295(3A).

³⁰ Commencing from years beginning 1 January 2025, certain entities will be required to report climate-related information. Refer Chapter 18 for further information.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ASIC Regulatory Guide 230 – 'Disclosing non-IFRS financial information' outlines financial information presented other than in accordance with accounting standards (i.e. non-IFRS financial information) and sets out guidance on how to use 'underlying profit' and other non-statutory financial information disclosure.

DIRECTORS' REPORT

The directors must prepare a directors' report made in accordance with a resolution of the directors, which is signed by a director.³¹ The directors' report requirements are dependent on the nature of the company.³² The required reporting obligations will vary for companies which are listed, limited by guarantee, large proprietaries and listed or unlisted registered schemes.

For listed entities, the annual remuneration report must be included in the directors' report, detailing the remuneration arrangements, payments and policies for directors and other key management personnel.³³ The remuneration report is subject to a non-binding advisory vote at the AGM by shareholders, however, there are consequences of an 'against' vote on the remuneration report following the introduction of the 'two-strikes' rule in 2011. This gives shareholders a right to vote on a board spill resolution if 25 percent or more of 'no' votes are recorded against the company's remuneration report in two successive AGMs. Generally, information that would unreasonably prejudice the company need not be disclosed in the directors' report (although if material is omitted, the report must say so).³⁴ When considering if the unreasonable prejudice exemption is available, directors should refer to ASIC's Regulatory Guide 247 – Effective disclosure in an operating and financial review.³⁵

Amongst other disclosures, a listed entity must give details of its operations, financial position, business strategies and prospects

³¹ Corporations Act, Section 298.

³² Corporations Act, Section 300A – regarding specific information to be provided by listed companies.

³³ Corporations Act, Section 300A.

³⁴ Corporations Act, Section 299(3).

³⁵ ASIC, 2019, Regulatory Guide 247 (RG 247) – Effective disclosure in an operating and financial review, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-247-effective-disclosure-in-an-operating-and-financial-review/>

for future financial years. ASIC's Regulatory Guide 247 – Effective disclosure in an operating and financial review, sets out guidelines for these disclosures.³⁶

DIRECTORS' DECLARATION

The directors' declaration³⁷ should include a solvency statement and mention of whether the financial statements and notes have been prepared in accordance with the Australian Accounting Standards, International Financial Reporting Standards, the Corporations Act, and provide a true and fair view of the financial performance of the entity for that reporting year. For financial years commencing on or after 1 July 2023, the director's declaration for public companies (both listed and unlisted) is expanded to include a declaration that the consolidated entity disclosure statement is in their opinion, true and correct at the end of the financial year. For listed entities, a resolution must be passed by the directors before the declaration is signed by a director (most commonly the chairman). Before the declaration is made, both the CEO and CFO must also give a declaration³⁸ regarding the veracity of the financial statements and notes and, in accordance with Recommendation 4.2 of the ASX Principles, certify that in their opinion it has been formed on the basis of a sound system of risk management and internal control which is operating effectively. The ASX Principles also extend this obligation of CEOs and CFOs to the financial statements for any period, not just the financial year.

When forming its opinion on the solvency of the company for the directors' declaration, a board is obliged to consider the debts of the company as at the date of the statement, not merely those debts included in the balance sheet as at balance date. ASIC believes the directors' declaration should contain a prospective element encompassing expected future debts that will compete for payment with existing debts. For this reason, directors should obtain all relevant information so that they can form an opinion about the company's solvency.³⁹

³⁶ *ibid.*

³⁷ Corporations Act, Section 295(4).

³⁸ Corporations Act, Section 295A.

³⁹ ASIC, 1992, Regulatory Guide 22 (RG22) – Directors' statement as to solvency, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-22-directors-statement-as-to-solvency/>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The basis of a board's resolution on solvency should be minuted. If all directors do not support the resolution, the resolution should indicate this fact. Those dissenting from the resolution should be identified and their reasons stated. A board may qualify its statement. This could occur, for example, if there is a material uncertainty about the company's ability to renegotiate loans for repayment. A qualified statement will not of itself limit the liability of directors, nor will it operate as a substitute for the proper discharge of their duties.

When a holding company wants to take advantage of the ASIC legislative instrument giving accounts and audit relief to wholly-owned subsidiaries, the directors of the holding company must consider the solvency of the entire group of companies subject to the class order, not just that of the holding company.⁴⁰

AUDITOR'S REPORT

An auditor must report to members on whether the auditor is of the opinion that the financial report is in accordance with the Corporations Act, including compliance with Australian Accounting Standards and International Financial Reporting Standards, and that the financial report provides a true and fair view of the financial position and performance for the financial year.⁴¹

The auditor's report must also describe any defect or irregularity in the financial report and any deficiency, failure or shortcoming relating to:

- obtaining all information, explanations and assistance necessary for the conduct of the audit
- keeping sufficient financial records to enable a financial report to be prepared and audited
- keeping other records and registers required by law.⁴²

⁴⁰ ASIC, Relief for wholly-owned entities under ASIC Corporations (Wholly-owned Companies) Instrument 2016/785, <https://asic.gov.au/regulatory-resources/financial-reporting-and-audit/preparers-of-financial-reports/relief-from-corporate-finance-provisions-including-for-wholly-owned-entities/>

⁴¹ Corporations Act, Section 308.

⁴² Corporations Act 2001, Section 307B and Section 308(3).

The auditor must also provide the directors with a written declaration as to the auditor's independence.⁴³ Most commonly, this declaration is carried over to the annual report for inclusion within the directors' report.

For general purpose financial reports of listed entities, the auditor's report describes key audit matters. Key audit matters are those matters that, in the auditor's professional judgement, were of most significance in the audit of the financial report of the current period. Key audit matters are selected from matters communicated with those charged with governance.

OTHER DISCLOSURES IN THE ANNUAL REPORT

The ASX Listing Rules require listed entities to produce a corporate governance statement which describes the extent to which an entity has followed the recommendations set out in the ASX Principles during the relevant reporting period.⁴⁴ The ASX Principles are not prescriptive, but a company that does not follow the recommendations must explain why, on an 'if not, why not' (or 'report or explain') basis. A company can publish its corporate governance statement in its annual report or provide a link to where the statement is located, or otherwise provide a separate copy of its corporate governance statement to the ASX at the same time that it provides its annual report.⁴⁵ In addition to providing its corporate governance statement (whether in the annual report or otherwise), a listed entity must also provide an Appendix 4G at the same time as it provides its annual report. The Appendix 4G serves a dual purpose. It acts as a key designed to assist readers to locate the governance disclosures made by a listed entity in its corporate governance statement and also acts as a verification tool for listed entities to confirm they have met the disclosure requirements of ASX Listing Rule 4.10.3.⁴⁶ In addition to statutory disclosures, many companies include additional information in their annual reports, such as overviews of business strategies and key drivers, and non-financial performance measures, and they convey these areas using snapshots, charts, artwork and photographs.

⁴³ Corporations Act 2001, Section 307C.

⁴⁴ ASX Listing Rule 4.10.3.

⁴⁵ ASX Listing Rule 4.7.4.

⁴⁶ ASX Listing Rule 4.7.4, See also ASX Guidance Note 9: Disclosure of Corporate Governance Practices, paragraph 8: The Requirement for an Appendix 4G.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Whilst often published under a separate report, many organisations are moving towards using the annual report to disclose their ESG achievements and compliance record, and to report on ESG initiatives. Commencing from years beginning 1 January 2025, certain entities will be required to report climate-related information in their annual reports.

In approving the content and format of annual reports, boards should keep in mind the following points:

- as far as directors are concerned, the annual financial reporting parts of annual reports are legal documents⁴⁷ – compliance with the legal requirements remains a key consideration for any board
- awareness of annual reporting 'best practice' for the nature and extent of disclosure, and for the presentation of information
- good reports usually incorporate a straightforward, logical and accurate account of the company's performance, together with a simple explanation of how the company intends to tackle the opportunities and problems confronting it
- whether it is more suitable to make the annual report readily available online or to distribute hard copies to shareholders.

The auditor's responsibilities with regard to other financial or non-financial information (other than the financial report and the auditor's report thereon) included in an entity's annual report are to read this other information and consider whether there is a material inconsistency between this other information and the financial report and the auditor's knowledge obtained in the audit.

CONCISE VERSION OF ANNUAL REPORTS

The Corporations Act permits all companies to distribute to shareholders 'concise versions' of their annual reports.⁴⁸ The concise report must be prepared in accordance with AASB 1039 Concise Financial Reports, and must contain some discussion and analysis of the position and results of the company to accompany the concise financial statements.

⁴⁷ Corporations Act 2001, s 295–300.

⁴⁸ Corporations Act, Section 314(1)(b) and Section 314(2).

The concise report must be audited and a full report must be provided to members if they request it.⁴⁹ This form of delivery is less common due to the availability of critical reports on the company website.

HALF-YEAR REPORTS

A disclosing entity must prepare a financial report and directors' report for each half-year and have the financial report audited or reviewed.⁵⁰

The half-year report may be either reviewed or audited, although in Australia a half-year report would only be audited in exceptional circumstances. Accordingly, the level of assurance provided by the auditor is dependent on the directors' choice.

	Half-year review	Half-year audit
Level of assurance	Limited	Reasonable
Scope of work completed	Lower	Higher
Type of work completed	Generally extends only to inquiry of management and analytical procedures on financial information.	Extensive. Includes evaluating accounting systems, testing and obtaining third-party evidence.
Risk of not detecting errors	Greater	Lower

AUDIT

An audit (as opposed to a review) is an examination of financial information. It is designed to obtain sufficient, appropriate evidence so the auditor can express a positive opinion that the financial report provides a 'true and fair' view of the company's financial position and performance.

⁴⁹ Corporations Act, Section 314.

⁵⁰ Corporations Act, Section 302.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The auditor draws on evidence from company and external sources, using, where appropriate, the company's internal controls and results obtained from substantive procedures. An audit provides a high, but not absolute, level of assurance on the financial information.

A review (as opposed to an audit) indicates that, based on the limited procedures performed, nothing has come to the attention of the auditor that indicates the financial report does not comply with the law. A review adds some degree of assurance to the financial statements, although considerably less than the level achieved by an audit.

The auditor must also describe any defect or irregularity in the financial report and any deficiency, failure or shortcoming relating to:

- obtaining all information, explanations and assistance necessary for the conduct of the audit
- the keeping of financial records sufficient to enable a financial report to be prepared and audited
- the keeping of other records and registers required by the law.⁵¹

Where applicable, the auditor must provide details of why the financial report does not so comply.⁵²

AUDIT COMMITTEE

Listing Rule 12.7 requires ASX listed companies included in the S&P/ASX 300 index to have an audit committee. The ASX Principles also suggest that a listed entity have an audit committee.⁵³ Audit committees are discussed in detail in Chapter 10, however, some information is included below in relation to the audit committee's role in the matters addressed in this chapter.

Boards should ensure that the internal governance systems include adequate involvement of the external auditor, internal audit and the board audit committee. The terms of reference of the audit committee should include a role in the review of significant corporate reporting, including financial disclosures before sign-off by the full board.

While the existence of an audit committee does not alter the need for directors to take responsibility for the financial reports, with the ultimate responsibility for a company's financial statements resting with the board, audit committees can play an important role in the financial reporting process and in supporting and promoting audit quality.⁵⁴ A separate audit committee can be an efficient and effective mechanism to bring the transparency, focus and independent judgement needed to the corporate reporting process.

The audit committee typically focuses on a limited range of key issues for statutory reporting purposes. It should review:

- any significant accounting and reporting issues, including professional and regulatory announcements, and understand their effect on the company's financial statements
- all half-year and annual financial statements of the company, and any other periodic disclosures, that require approval of the board (the process typically culminates in a detailed page-by-page review by the audit committee of these reports with the external auditor and management present)
- the written statements provided by the CEO and CFO for Australian reporting purposes (under s 295A of the Corporations Act and Recommendation 4.2 of the ASX Principles)
- the processes, policies and procedures for compliance with the company's continuous disclosure obligations
- all related party transactions for potential conflicts of interest, providing approvals on an ongoing basis.

The commentary to Recommendation 4.1 of the ASX Principles sets out the role of the audit committee and the matters which it should consider and make recommendations to the board.

⁵¹ Corporations Act, Section 309.

⁵² Corporations Act, Section 309(4) and (5).

⁵³ ASX Corporate Governance Principles and Recommendations, 4th Edition, Recommendation 4.1.

⁵⁴ ASIC Information Sheet 196 (INFO 196).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

CONTINUOUS DISCLOSURE

Disclosing entities (both listed and unlisted) are subject to continuous disclosure requirements. Unlisted disclosing entities should refer to ASIC's *Regulatory Guide 198 – Unlisted disclosing entities: Continuous disclosure obligations* for guidance on complying with their continuous disclosure requirements and also Section 675 of the Corporations Act. The continuous disclosure requirements of ASX listed entities are governed by the ASX Listing Rules and also Section 674 of the Corporations Act.

Pursuant to ASX Listing Rule 3.1,⁵⁵ a listed entity must immediately notify the ASX once it becomes aware of any information concerning it that a reasonable person would expect to have a material effect on the price or value of the entity's securities, subject to the carve-outs to immediate disclosure set out in Listing Rule 3.1A.

Under Listing Rule 3.1B, if ASX considers that there is, or is likely to be, a false market in the company's securities, then ASX may require the company to give ASX any information it asks for to correct or prevent that false market. The term 'false market' refers to a situation where there is material misinformation or materially incomplete information in the market which is compromising proper price discovery. This may arise, for example, where there is false or misleading information circulating in the market, including a specific rumour or media comment affecting the company's share price.⁵⁶

The ASX Principles recommend that companies establish and disclose written policies and procedures designed to ensure compliance with ASX Listing Rules disclosure requirements and to ensure accountability at a senior executive level for that compliance.⁵⁷

Each board should establish and approve policies and procedures to ensure the company complies with continuous disclosure requirements and that this is linked with the spokesperson policy. Commentary to Recommendation 5.1 of the ASX Principles contains useful information for consideration when formulating a continuous disclosure policy. The policies and procedures for meeting the continuous disclosure requirements should be made publicly available, ideally by posting them on the company's website. A 'balanced' approach to disclosure in reporting both positive and negative information should also be considered.

There are other channels aside from the ASX company announcements platform that facilitate reporting to the market. These include the company's investor presentations, roadshows, annual reports and the company's website. However, it is important to note that where any market-sensitive information is proposed to be released to a section of the market (for instance, at an investor or analysts' briefing), such information must **first** be provided to the ASX in accordance with Listing Rule 3.1 before it can be released via any other channel.

Information is considered to be 'generally available' if: it consists of readily observable matter; or it has been made known in a manner that would, or would be likely to, bring it to the attention of people who would commonly invest in the relevant securities and, since it was made known a reasonable period for it to be disseminated among such people has elapsed; or it otherwise consists of deductions, conclusions or inferences made or drawn from such matters.⁵⁸ The ASX carefully monitors the interaction between disclosure and movements in either volume or the price of shares to identify aberrations that suggest either manipulation or deficient information to the market.

Guidance Note 8 – Continuous Disclosure: Listing Rules 3.1 – 3.1B clarifies the approach of ASX to interpreting and enforcing the continuous disclosure requirements under ASX Listing Rule 3.1, and when the ASX may refer a possible breach of that rule to ASIC.⁵⁹

⁵⁵ Corporations Act 2001, s 674 – requires listed disclosing entities to comply with ASX Listing Rule 3.1 on continuous disclosure.

⁵⁶ ASX Guidance Note 8: Continuous Disclosure: Listing Rules 3.1 – 3.1B, Section 6 Listing Rule 3.1B – correcting or preventing false markets.

⁵⁷ ASX Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 5.1.

⁵⁸ Corporations Act, Section 676(2).

⁵⁹ ASX Guidance Note 8, Section 4.5: The meaning of 'immediately'.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

In addition, the Guidance Note clarifies, among other things, the meaning of 'immediately', the 'reasonable person' test, earnings guidance and surprises, and the use of trading halts to manage disclosure issues.

Under Guidance Note 8, the meaning of 'immediately' is defined as meaning 'promptly and without delay', that is doing something as quickly as it can be done in the circumstances (acting promptly) and not deferring, postponing or putting it off to a later time (acting without delay).

There are criminal and civil penalties for breach of the continuous disclosure requirements. Directors may also contravene their duty of care and diligence⁶⁰ by not complying with the continuous disclosure obligations.

2021 changes to continuous disclosure laws

The Treasury Laws Amendment (2021 Measures No. 1) Bill 2021 was passed on 13 August 2021. This Bill seeks to permanently amend the continuous disclosure obligations in the *Corporations Act 2001* (Cth) (Corporations Act) such that companies and their officers will only be liable in civil proceedings for alleged breaches of continuous disclosure obligations, where they have acted with 'knowledge, recklessness or negligence'.

The Bill introduces sections 674A and 675A into the Corporations Act and in summary specifies that companies and their officers who have prima facie contravened continuous disclosure requirements will not be liable for misleading and deceptive conduct (under sections 1041H of the Corporations Act and 12DA of the *Australian Securities and Investments Commission Act 2001* (Cth)) unless it can be proven that the company or officer acted with 'knowledge, recklessness or negligence'.

The reforms are only in place for two years at which point a review by an independent expert is required to be undertaken. Action at that point will determine whether the reforms expire or are made permanent in their current form or with some amendment.

⁶⁰ Corporations Act 2001, s 180 (1). Also refer to [Chapter 1](#) for more information about directors' legal duties and obligations.

It is hoped that the reforms will provide more confidence to directors on making disclosures to the markets without the fear of class action looming as a disincentive. However this bill does not change ASIC's ability to prosecute under ASX Listing Rule 3.1.

Ultimately, these changes shouldn't change the manner in which entities (and directors) ensure that continuous disclosure requirements are met. The same level of rigour and due diligence should be applied with clear records being maintained.

INVESTOR DECISION-MAKING

If companies are to maximise returns to their shareholders, they must not only create value, but be seen to have created value and provide prospects for value creation in the future. This is essentially a matter of communicating with shareholders, potential shareholders and third parties in a position to influence investors' share buying, retention and selling decisions.

Regular and effective reporting and communications between the company and these parties influences the decision-making of shareholders and potential investors.

It is, however, widely acknowledged that traditional information flows (e.g. general purpose statutory financial reporting) and engagement practices (e.g. AGMs) do not typically address the broad range of issues of concern to individuals and entities seeking to make timely, accurate and precise decisions on their investments, or potential investments, in the company. Therefore, companies need to address the limitations of traditional reporting to fulfil their intended purpose and seek ways to better inform investors.

A more contemporary model of business reporting and communication that creates reports based on what the company wants to communicate – and on what investors want and need to know – can ensure that shareholders will make the right decisions, at the right time, about the things that matter to the company, particularly investment opportunities. Reporting and communication

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

strategies should be directed to balancing the performance/reward equation and aligning business rewards – capital, licences to operate (including social licence) and reputation – with company performance.

Integrated reporting of this kind takes a more forward-looking and holistic approach to articulate the organisation's:

- business strategy
- performance in executing the strategy
- insights about the drivers and risks threatening the successful execution of the strategy
- outlook for future performance if the strategy is well executed.

This model implies specific reporting on performance drivers, such as infrastructure, people, business processes, strategic management, risk management and governance performance, and the dynamic interplay between all of these factors.

Through integrated reporting, shareholders can gain an appreciation of the strength of the business model in terms of its:

- velocity (speed of business processes)
- vulnerability (to shocks from business risks)
- versatility (flexibility and agility in the face of changing external forces and market conditions)
- volatility (consistency of business processes in the face of change).

With integrated reporting, companies can also provide more detail and clarity over the broader health of the organisation and the challenges and opportunities it faces in the future, rather than just a summary and discussion on historic financial results. Integrated reports provide a clearer understanding of how the organisation creates and preserves sustainable value by focusing on governance, resource use and exposure, short, medium and longer term risk to value, and how they are being addressed, as well as strategic performance and future outlook.

In contrast to this, in traditional reports, the reader is not given sufficient information to assess a company's ability to execute its strategy in the future and whether past earnings are likely to be sustainable in the medium to long term.



FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

THE BOARD'S ROLE IN BUSINESS REPORTING

Business reporting should accurately reflect and communicate the real corporate picture. Boards are in a unique position to step back from the day-to-day perspective of management and view the organisation from all perspectives. Boards should be able to assist in improving the quality of reporting by identifying any major gaps between what is being reported to shareholders and investors by management and what should be reported, whilst having regard to stakeholder needs, concerns, influences and decision-making behaviour.

Thus boards are actively seeking a new reporting framework to help them decide on what to report, when, to whom, in what format and why. However, there are many impediments to change, including:

- the risk of litigation if forward-looking statements are not met
- the release of competitively sensitive information or information that may be subject to rapid change or volatility
- a lack of willingness on the part of competitors and industry participants to be more forthcoming with voluntary disclosures
- no agreed industry reporting standards
- concern that capital markets will not cope with/synthesise the extra information
- markets being only interested in short-term performance.

There are a number of ways to improve business reporting, including:

- encouraging more direct involvement by the board
- aligning internal reporting with external reporting (statutory reporting, results announcements and investor presentations, corporate social responsibility reporting, and other more frequent reporting such as:
 - pro forma/non-GAAP earnings guidance, production reports or balanced scorecards looking at the performance of non-financial KPIs
 - improving consistency and clarity in the company's message (strategic goals/objectives) and the linkages between financial and non-financial reporting
 - streamlining reporting and creating a balanced portfolio of reports
 - educating shareholders on the implications and value of reporting changes
 - using technology for reporting automation and diffusion (e.g. XBRL, web-based and real-time reporting, enterprise and data modelling).

The ASX Principles and Recommendations include a corporate reporting process recommendation, sitting within Principle 4, requiring disclosure of the process to validate corporate reports and to provide investors with appropriate information to make informed investment decisions (Recommendation 4.3). The commentary to the corporate reporting process recommendation notes that some entities use the principles of integrated reporting as a useful framework for preparing operating and financial reviews in director reports.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- ASIC, 2012, Regulatory Guide 73, Continuous Disclosure Obligations: Infringement Notices, <http://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-73-continuous-disclosure-obligations-infringement-notice/>
- ASX Guidance Note 8: Continuous Disclosure: Listing Rule 3.1 – 3.1B, https://www.asx.com.au/documents/rules/gn08_continuous_disclosure.pdf

For further information please contact:



Kim Heng

Partner, Audit & Assurance
KPMG Australia
kheng@kpmg.com.au



Peter Trace

Partner, CFO Advisory
KPMG Australia
ptrace@kpmg.com.au

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

8. Stakeholder Engagement

Stakeholder expectations have undergone rapid change and continue to do so. Effective stakeholder engagement is critical to risk management and organisational sustainability. Boards and directors need to understand and respond to stakeholder issues and needs, and incorporate stakeholder perspectives into planning and decision-making.

In this chapter

- Defining stakeholder engagement
- Why focus on engaging stakeholders?
- Stakeholder engagement at board level
- Stakeholder engagement and strategy development
- Establishing an effective stakeholder engagement framework

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Is the board comfortable that it knows who its key stakeholders are, including their interests, values and needs?
2. Does the organisation understand all material stakeholder issues and concerns?
3. Is the organisation aware of the risks associated with insufficient engagement – both risks to the organisation (including reputational, legal, financial and operational risks) and risks to people? If applicable, does the organisation quantify these risks?
4. Have stakeholders with the ability to influence strategic and operational decision-making, or organisation objectives and performance, been effectively engaged? Does the organisation effectively engage stakeholders who are, or may be, impacted by its activities?
5. Does the organisation have a stakeholder engagement framework aligned with best practice?
6. Does the organisation have a clear and approved policy, process, plan, and narrative for engaging with stakeholders?
7. Is the purpose of stakeholder engagement defined and well-understood across the organisation?
8. Is stakeholder engagement embedded within the organisation's vision, mission, and strategy statements?
9. Does the organisation monitor stakeholder perception?
10. Does the organisation provide feedback to stakeholders, to share the outputs and learnings of its stakeholder engagement, and to inform stakeholders of the next steps it will use to act on feedback received?
11. Does the board seek and maintain relationships with its key stakeholders at the leadership level?
12. Does the organisation publicly report on its commitment, approach, and performance in stakeholder engagement?
13. Is stakeholder engagement used as a strategic mechanism to manage risk, rather than as a responsive tool?
14. Is there adequate organisational consideration of creating opportunities for stakeholders as well as managing risk?
15. Is there an anonymous feedback mechanism, beyond whistleblowing, available for stakeholders who frequently interact with the organisation?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The organisation does not maintain stakeholder mapping, prioritisation or profiling information.
- The organisation defines stakeholders narrowly as 'clients' and 'customers'.
- Vulnerable stakeholders, who have limited voice, are not considered but are impacted by or dependent on the organisation's activities and decisions.
- Stakeholders are not considered or consulted in decision-making unless they are considered highly influential.
- The risk of insufficiently engaging stakeholders is not discussed or is dismissed by some board members.
- Dialogue with stakeholders mostly occurs in the event of disputes and negative media coverage.
- Online coverage of the organisation is mostly negative and/or the organisation is the subject of stakeholder activism.
- Leadership and board accountabilities for stakeholder engagement is unclear and/or there is no stakeholder management structure in place.
- There is a gap between internal facing and external facing organisational positions.
- Board members do not hold strong or effective relationships with a range of key stakeholders.
- Stakeholder engagement activities/outcomes are not tracked, monitored or reported on.
- Stakeholder interests, issues and perceptions about the organisation are unknown or undocumented, with no process to identify, review or anticipate risks associated with stakeholder perceptions.
- There is limited understanding of how the organisation's positions may potentially intersect with government or stakeholder interests and priorities.
- There is no clear commitment to, or process or systems in place for, engaging with stakeholders.
- The organisation does not have an up-to-date stakeholder engagement plan in place, and/or it does not include a specific strategy or process for engaging with Indigenous Peoples.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

DEFINING STAKEHOLDER ENGAGEMENT

Stakeholder engagement is the process of identifying and meaningfully involving the key groups of people and organisations who are affected by, or have the capacity to influence, an organisation's decisions, activities and operations.

Expectations regarding the extent to which relevant stakeholders participate in decision-making are continuing to develop. For example, the IAP2 Public Participation Spectrum¹ encourages organisations to consider the potential to collaborate with the public on decision-making or to even empower them to make final decisions, while the Indigenous right to free, prior and informed consent is articulated in the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP)² and requires genuine and significant decision-making involvement.

Traditionally, a board's direct involvement with its key stakeholder groups has been limited to the chair, or the respective chairs of committees such as the audit committee or the sustainability committee. In extraordinary circumstances, the wider board may have become involved in engagement activities and communication.

Today, however, management is regularly turning to directors to tap into their expertise and relationships to facilitate engagement, advocacy and lobbying with key stakeholders. Directors who possess 'change agent' competencies can be influential in championing particular courses of action.

Even when a board is not directly involved in stakeholder engagement, they are key to providing the 'tone from the top' and have a vital role to play in ensuring both good governance and that an organisation's commitment to engage meaningfully with stakeholders is met.

- 1 International Association for Public Participation (IAP2), Public Participation Spectrum, (Online Resource, 2014), https://iap2.org.au/wp-content/uploads/2019/07/IAP2_Public_Participation_Spectrum.pdf
- 2 United Nations Declaration on the Rights of Indigenous Peoples, GA Res 61/295, UN Doc A/RES/61/295 (2 October 2007, adopted 13 September 2007).

WHY FOCUS ON ENGAGING STAKEHOLDERS?

A good corporate reputation is a prized asset earned over time. It can be a source of competitive advantage. However, organisations now exist in an environment of heightened scrutiny from various stakeholders over the sustainability and integrity of their operations. Companies perceived as acting in a detrimental fashion are exposed not just to reputational risk, but also to legal, operational and commercial risk. In contrast, companies that engage meaningfully with their stakeholder base can benefit from well-considered decision-making, greater accountability and a more positive public image.

Moreover, investors, lenders and clients/customers (including governments) are increasingly assessing an organisation's fulfilment of sustainability, community relations and other stakeholder engagement criteria for investment, lending and contracting decisions. Effective stakeholder engagement processes are essential in order to be able to demonstrate to these other actors in the value chain that these requirements are fulfilled.

Examples from beyond Australia highlight potential future stakeholder engagement requirements. Corporate governance reform in the UK includes requirements for boards to understand and report on how stakeholders' interests have been considered in board discussions and decision-making.³ The UK corporate governance regime is influential in Australia⁴ and may provide useful insight on the future of directors' duties with respect to stakeholders in Australia. Given the increased expectations of stakeholders and the potential risks if they are not adequately engaged, directors' duties should include avoidance of reputational risk. This requires significant oversight over the organisation's stakeholder engagement activities.

3 Refer to The UK Corporate Governance Code, July 2018, s5, <https://www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UK-Corporate-Governance-Code-FINAL.pdf>

4 Refer for example to the Financial Accountability Regime, 11 July 2024, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-279-financial-accountability-regime-information-for-accountable-entities/> This regime was heavily based on the UK's Senior Managers Regime.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

STAKEHOLDER ENGAGEMENT AT BOARD LEVEL

Organisations with effective stakeholder engagement possess a strong 'tone from the top'. Boards are responsible for setting the general policies and direction of the organisation. They shape the organisation's framework for accountability, and they should lead by example in fostering an outward-looking approach.

Meaningful stakeholder engagement should be a core organisational principle, set at board level. Directors should identify the key risks associated with evolving societal expectations and set requirements with their executive management group around effectively engaging the organisation's stakeholder base. Further, the board should also consider their own interface with their stakeholders, including the integration of stakeholder issues into the AGM and public reporting.

STAKEHOLDER ENGAGEMENT AND STRATEGY DEVELOPMENT

Stakeholders can provide a unique perspective on an organisation's performance, challenges, and opportunities. Strong and effective stakeholder engagement provides boards with a range of views that might otherwise be missed in strategy development and risk assessment processes.

A robust strategy development process involves exploring the macro and micro environment for current and emerging issues that could impact the organisation's operating model. Management and the board tend to have a good grasp of the local/micro influences. However, having the perspective of stakeholders' external lens can provide the organisation with a unique input to inform strategy development and the identification of risks and opportunities.

The AA1000 AccountAbility principles include the concept of materiality. While materiality has traditionally been used in the context of financial reporting, today materiality is used to encompass the 'needs, interests and priorities' of an organisation as well as of its stakeholders.⁵ The concept of double materiality outlined by the Global Reporting Initiative (GRI) – encompassing consideration of both financial materiality (i.e. financial value creation) and impact

materiality (i.e. impacts on the environment and society) – further emphasises the increasing relevance of stakeholder perspectives to organisations' decision-making and risk management.⁶

ESTABLISHING AN EFFECTIVE STAKEHOLDER ENGAGEMENT FRAMEWORK

To be effective, organisations require formalised stakeholder engagement strategies, plans and processes. A stakeholder engagement framework can help facilitate a consistent, integrated, and effective approach. A stakeholder engagement framework may include:

- Objectives, scope (including boundaries of disclosure) and guiding principles of engagement.
- Stakeholder models/maps, profiling, and prioritisation.
- Responsibilities for developing and managing stakeholder engagement (including agreed accountabilities for the board and management).
- Engagement levels and methods, including methods of informing stakeholders, gathering feedback and perspectives, and partnering.
- Methods and accountabilities for monitoring and measuring stakeholder concerns, influences and sensitivities, e.g. surveys.
- Methods for monitoring and evaluating stakeholder engagement activities and the implementation of the framework.
- Established positions on relevant public or industry specific policies.
- Methods of, and a commitment to, reporting back a summary of stakeholder feedback and next steps.

The AA1000 series of Stakeholder Engagement Standards provide an internationally recognised framework to help organisations ensure that their stakeholder engagement processes are purpose-driven, robust and deliver results, and form a basis for designing and implementing effective stakeholder engagement in a credible way.⁷

⁵ AA1000 AccountAbility Principles 2018, <https://www.accountability.org/standards/aa1000-accountability-principles/>, p. 21.

⁶ GRI, 'Understanding materiality can unlock accountability', 22 February 2022, <https://www.globalreporting.org/news/news-center/understanding-materiality-can-unlock-accountability/>

⁷ For further information refer to AA1000, 2015, Stakeholder Engagement Standard, <https://www.accountability.org/standards/aa1000-stakeholder-engagement-standard/>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Trustworthy by design

Trust is best defined as the willingness to be vulnerable to the actions of another party based on positive expectations of the intentions or behaviour of that party.

A company's reputation for trustworthiness is influenced by the trust held throughout its stakeholder ecosystem, including customers, employees, investors, suppliers and partners, regulators and policymakers, communities influenced or impacted by its operations – citizens and the general public.

Stakeholders trust organisations they perceive to have three key characteristics:

- **Ability** – 'I can rely on you to be competent': the collective knowledge, skills, and competencies that enable the organisation to function reliably and effectively to deliver its products and services and meet its goals and responsibilities. Ability is specific to the domain requiring trust. We may trust an organisation in one way (e.g. for high quality products), but not in another (e.g. for efficient customer service).
- **Humanity** – 'I believe you care about your stakeholders': exercising benevolence and a duty of care to those affected by the organisation's operations, products, and services. At a minimum this means doing no harm. More broadly, humanity involves having a positive orientation towards stakeholders that goes beyond a profit motive and creates value for them.
- **Integrity** – 'I trust you to do the right thing': consistent adherence to commonly accepted ethical principles and moral values, such as honesty, fairness, promise fulfilment, responsibility for one's actions, and operating within the law. Integrity is also demonstrated by living expressed values.

Research indicates that if any one of these characteristics is missing it undermines perceptions of trustworthiness.

(Source: KPMG and the University of Queensland Business School, 2019, *Trustworthy By Design*)

STAKEHOLDERS

Organisations' stakeholders differ depending on the nature, size, and complexity of the organisation, however, stakeholders common to most organisations include:

- i. Community, including Indigenous communities
- ii. Employees
- iii. Customers and consumers
- iv. Suppliers
- v. Investors and shareholders
- vi. Financiers
- vii. Regulators and government – local, state, federal
- viii. Civil society, multi-stakeholder bodies and NGOs
- ix. Media

I. Community, including Indigenous communities

Identifying, understanding and engaging with communities who are potentially affected or impacted by, close to, or interested in an organisation's activities is a minimum requirement in today's landscape. Having a clear and direct approach to informing, consulting and partnering with community groups has never been more important.

Community engagement is key to building and maintaining community trust and a social licence to operate (SLTO). SLTO refers to the gaining and maintaining of support for a sector, organisation or project and their associated activities, and reflects the beliefs, perceptions and opinions held by the community and stakeholders. It is dynamic and can evolve based on the quality of communication and engagement, the actions of a sector, organisation or project, the impact of these actions on a community or stakeholders, and the influence of other issues influencing the community. Loss of trust, acceptance or SLTO can have significant reputational, legal and financial implications.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Engaging with Indigenous communities requires specific considerations. The engagement approach should be agreed with the community beforehand, and engagement should be culturally appropriate and conducted by culturally competent people. The Indigenous right to consultation and free, prior and informed consent (FPIC) should be embedded into the process and the unique knowledge, experience and skills of Indigenous stakeholders should be respected and included in decision-making.

Directors can undertake the following actions to help their organisation engage with their community stakeholders:

- Requesting a report from management on the organisation's key community groups and the current engagement activity. Understanding the community's needs, issues, and priorities.

- Assigning accountability for directors to engage and own the relationship between key community groups.
- Developing community stakeholder engagement strategies and plans, with a separate strategy for Indigenous stakeholders that is culturally appropriate and respectful of their rights.
- Ensuring community stakeholders are engaged as part of the organisation's product/service/project development process, and during instances where there are significant planned changes.
- Ensuring community stakeholder feedback is reported to the board.



Case study: South West Renewable Energy Zone, NSW

Early community consultation on renewable energy in Hay Shire, within the South West Renewable Energy Zone has led to little to no local objection to renewable energy projects, and better outcomes for local residents.

Community consultation, led by the Hay Shire Council set 'rules of engagement' for all stakeholders seeking to develop renewable energy projects in the area, ensuring the transition occurred 'with us, not to us'.

One result of the community consultation process in Hay was greater community acceptance of renewable energy projects in the region. One of the largest projects from French multinational Engie proposes hybrid wind, solar and battery storage. The company's development manager Aref Taleb said that while there has been vocal opposition to renewable energy projects in other parts of the state, there had been no local objections in Hay, which is 'extremely rare for energy projects in the country' according to Mr Taleb. Mr Taleb observed that the community is 'extremely open to new, innovative ideas for how they can sustain the region long term'.

The engagement approach has also seen better community outcomes, with Hay residents and economy receiving a greater share of the benefit and seeking more than just an 'economic sugar hit' from project construction. Instead, there has been a long-term focus on education, housing, healthcare, and cheaper electricity for residents. For example, the community have been able to negotiate \$1,000 rebates per year for 30 years for anyone living within 20 km of a project, and vouchers for anyone within the LGA.

Learn more

ABC News, [Renewable wind and solar farms on the Hay Plain in NSW to boost economy, build sustainable farms](#)

Hay City Council, [Fundamental Principles for Successful Renewal Development in Hay LGA](#)

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ii. Employees

To build a high-performing culture that delivers the organisation's purpose and promise to all its employees, directors need to consider the following culture drivers:

- Leadership
- Purpose
- Values and behaviours
- Communication
- Governance
- Capability
- Structure
- Systems and processes.

For employees, job satisfaction usually requires:

- fair remuneration and compensation
- a safe, healthy, and respectful workplace
- job security
- professional and personal development
- respect, recognition and acknowledgement
- alignment to the organisation's purpose and strategy
- open and honest communication
- a culture and process that supports psychosocial safety, to support employees to speak up, when required.⁸

Through corporate governance, boards often have a direct impact on employee interests. For example, boards will help establish, review, and approve the management and employee remuneration structure. Similarly, boards help set and maintain an organisation's culture, which in turn influences key job satisfaction factors, such as transparency of communication with employees and reward and recognition.

⁸ Employers have a positive duty to prevent workplace sexual harassment, sex-based discrimination and victimisation. Read more here: [Eliminate sexual harassment | Respect@Work – KPMG Australia](#)

Finally, risky decision-making at the board level may impact on the overall level of job security an organisation can offer employees.

Directors can undertake the following actions to help their organisation support and engage with their workforce:

- Clearly defining and communicating the organisation's purpose and values.
- Placing a priority on workplace health and safety, including psychosocial safety.
- Ensuring there is a genuine commitment to diversity, equity, and inclusion.
- Ensuring there is an appropriate grievance mechanism and that grievances are responded to appropriately.
- Investigating whether individual grievances are linked to widespread/cultural issues that need to be addressed.
- Encouraging the use of employee surveys and taking accountability to ensure that feedback and recommended next steps, and progress on those actions, are shared with employees to build employee trust.

iii. Customers and consumers

For businesses that operate direct to consumer (B2C), customers play a fundamental role in securing revenue for a business, with customer acquisition and retention key to the bottom line. To keep pace with growing customer expectations, organisations are moving toward customer-centric models of operation, which require alignment and integration across an organisation's functions, across back, middle and front of office.

Organisations that do this effectively are 'connected enterprises'. These organisations are characterised by customer-centric approaches, making data-driven decisions, empowered workforces, and secure, agile technology architectures that support innovation. They tend to deliver customer excellence and superior customer experience across all touchpoints.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Defining back, middle and front office

- **Back office:** the administrative and support tasks that are essential for the smooth operation of the organisation but do not involve direct customer interaction. This includes functions such as accounting, IT, human resources, and logistics.
- **Middle office:** the bridge between the front office and back office. It focuses on risk management, compliance, and ensuring that transactions and operations initiated by the front office are executed correctly and efficiently. The middle office also handles financial control, strategy, and performance management.
- **Front office:** the front office is primarily responsible for direct interaction with customers and clients. This includes activities such as sales, customer service, marketing, and support. The front office is the face of the organisation and is crucial for generating revenue and maintaining customer relationships.

Customer experience excellence entails delivering a consistently superior experience that meets or exceeds customer expectations across all touchpoints through The Six Pillars of customer experience:

- **Personalisation:** demonstrating an understanding of the customer's specific needs, circumstances, and aspirations, and tailoring the experience accordingly. This makes customers feel valued and important.
- **Integrity:** building trust through consistent and trustworthy organisational behaviour. This involves delivering on promises and having a strong sense of purpose beyond just making money.
- **Expectations:** understanding, meeting, and ideally exceeding customer expectations. This requires clear communication and setting realistic yet ambitious goals.
- **Resolution:** efficiently addressing and resolving any issues or problems that arise. This includes making customers feel good about the resolution process through sincere apologies and urgent actions.

- **Empathy:** showing an emotional understanding of the customer's experience. This involves behaviours that reflect to the customer that their feelings are understood and considered.
- **Time and Effort:** minimising the effort required by customers to achieve their objectives. This involves removing unnecessary obstacles and making processes as straightforward as possible.

Directors may undertake practical measures to ensure the organisation is appropriately engaging and managing its customer relationships by:

- Bringing visibility of customer satisfaction data and insights to directors through regular, robust and relevant reporting. This is known as a Voice of Customer program, and is sometimes driven in a business by a 'Customer Advocate' role.
- Having a view of the 'customer journeys' across the various products or services the business provides. A customer journey plots the steps that customers take to access and consume an organisation's products or services, enabling the organisation to put themselves in the shoes of their customers to identify pain-points and gain-points that reduce or support customers' experiences
- Considering implementing customer satisfaction measures in the business's objectives and key results, and as key performance indicators for senior relevant staff.

iv. Suppliers

The responsibility of organisations to set clear standards for their suppliers and to undertake review or audit, is increasing, in part due to an increasing awareness of potential risks in organisation's supply chains. This awareness can be at odds with the traditional view of competitive business environments, where there is increased pressure to reduce costs while maintaining or improving the quality of the organisation's products and services.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Suppliers can be highly influential in the success (or otherwise) of an organisation. For example, an organisation that maintains a high profit margin at the expense of a key supplier that is struggling to maintain solvency may find itself in trouble long term. Similarly, any compliance, regulatory, legal and/or environment, social and governance (ESG) issues that impact a supplier will often have a negative reputational impact upon the procuring organisation, requiring a comprehensive approach to considering the needs of an organisation and its suppliers.

Organisations must take particular care when working with suppliers whose employees are at high risk of poor labour standards, modern slavery, or other labour rights violations. For example, in Australia, cleaning, hospitality and agricultural workers are considered some of the most at-risk, due to the intersection of lower standards of education and higher rates of migrant workforces, which can make these workers vulnerable to exploitation. The introduction of the *Modern Slavery Act 2018* (Cth)⁹ in Australia has required organisations to report on how modern slavery risk is managed in operations and supply chains.

Directors may undertake practical measures to ensure the organisation is appropriately engaging and managing its suppliers including:

- Having visibility over suppliers' business practices and understanding how the organisation's business model may influence supplier behaviour or incentives.
- Ensuring the organisation maintains robust procurement processes that incorporate not only value for money factors, but also long-term sustainability, labour standards, corporate reputation, and any history of involvement with business practices below the standard expected by the organisation.
- Ensuring the organisation establishes mechanisms to measure and monitor suppliers' adherence to ESG policies and standards, including those related to modern slavery and broader human rights.

For further information on directors' roles in ethical supply chains, see [Chapter 25 \(Human rights and modern slavery\)](#).

⁹ Modern Slavery Act 2018 (Cth), <https://www.legislation.gov.au/C2018A00153/latest/text>

v. Investors and shareholders

Directors have a duty to act in the best interests of a company, including for shareholders and investors. While director engagement with investors and shareholders is not a new concept, investor and shareholder expectations are rapidly shifting, particularly in relation to ESG and responsible investing. Maintaining a constructive relationship with investors provides valuable information to shape organisational responses to rapidly shifting expectations.

In 2023, Australia's responsible investment market was valued at \$1.6 trillion, or 41 percent of the investment market in Australia.¹⁰ These investors actively consider ESG factors in investment decisions, and acknowledge that these factors are critical to understanding current fundamental value and future value of an investment decision. Our Global ESG due diligence study 2024 found that in Australia and the Asia Pacific (ASPAC) region, 60 percent of investors would be willing to pay more for a target which demonstrates high ESG maturity.¹¹ Findings such as this makes it increasingly important that directors are attuned to ESG issues for their organisation, investor expectations for disclosure and management, and are appropriately managing ESG risks and opportunities. Directors are responsible if any material issue that may impact on the economic success or viability of the organisation has been mismanaged or ignored.

Proactive engagement with investors and shareholders can also mitigate shareholder activism. The Australasian Centre for Corporate Responsibility has reported that since 2024, ESG-related resolutions are on the rise, with 30 percent growth since 2020, compared to 2015–19. There have been 91 ESG-related resolutions put to Australian ASX 200 companies in the period since 2020.¹²

¹⁰ Responsible Investment Association Australasia (RIAA), 'Responsible Investment Benchmark Report', (2024), <https://www.responsibleinvestment.org/research-and-resources/resource/responsible-investment-benchmark-report-australia-2024>

¹¹ KPMG, 'Global ESG due diligence study', (2024), <https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2024/06/esg-due-diligence-study-2024.pdf>

¹² Australasian Centre for Corporate Responsibility (ACCR), 'Australian ESG Shareholder Resolutions', <https://www.accr.org.au/research/australian-esg-resolution-voting-history/>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Directors can engage with investors and shareholders on ESG in the following ways:

Role of directors with investor and shareholders	Questions to ask
Annual General Meetings – presenting not just results, but ESG performance and management.	– Do you understand the ESG data demands and queries and the material topics of interest to investors/financiers? – Is the company ready to respond to the ESG data demands and queries of investors and financiers?
Ensuring appropriate ESG disclosures as part of annual reporting suite and stock exchange disclosures.	– Do you understand what ESG disclosures your investors expect?
Direct engagement as part of one-on-one engagement, consultation, and investor days.	– What is your engagement plan over and beyond annual disclosures and AGMs? – Do you have oversight and direct engagement with large investors and institutional investors?
Understanding the material ESG topics for your business, consulting with and surveying investors on ESG topics of concern. Ensuring that appropriate management strategies are employed.	– Do you understand your organisation's material ESG topics including double materiality of these issues? – Do you understand the primary ESG topics of concern for your investors? Have these been determined via consultation with investors? – Do you understand the ESG data demands and queries of your investors? – Are you adequately equipped to answer questions from your investors relating to ESG?
Oversight of the investor relations functions.	– Do you have oversight of the investor relations functions and activities including their responses to investor surveys relating to ESG?
Setting ESG culture from the top and communicating the organisation's ESG story internally to employees and to investors externally.	– How do you actively maintain an ESG culture and story within your organisation?

For more information on directors' shareholder responsibilities refer to [Chapter 7](#).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US



Case study: Dhawura Ngilan Business and Investor Guide

The Dhawura Ngilan Business and Investor Guide recognises that businesses and investors have a responsibility to respect First Nations Cultural Heritage as an integral part of Australia's history and identity, and recognising the serious legal, financial, and reputational consequences if they fail to do so.

Developed in collaboration with investors, the guide provides resources to enable investors and businesses to achieve better practice through their strategies, operations, business and business relationships, and identifies red flags for investors when considering their company portfolio.

The guide advises that engagement with potentially affected First Nations rights holders and stakeholders should be ongoing, and investors should be responsible for monitoring this ongoing engagement within their investment profile. Therefore, directors should expect growing questions from investors on their management of engagement activities relating to First Nations and Cultural Heritage.

Organisations seeking to advance their own relationships and engagement with First Nations peoples should refer to the detailed guidance within the Dhawura Ngilan Business and Investor Guide.

Read more about the Dhawura Ngilan Business and Investor Principles and Guide: https://culturalheritage.org.au/wp-content/uploads/2024/03/DNBII_BusinessesInvestorsGuide.pdf

vi. Financiers

Similar to investor and shareholder expectations, the expectations of financiers such as banks and debt investors relating to ESG are expanding rapidly. Financiers are increasingly considering ESG as part of their decisions on whether to finance loans, and considering ESG risks within their loan book. Banks are facing increasingly complex requirements to report exposures to ESG risks (particularly related to climate change and transition) within their investment portfolio. This includes financial institutions transitioning their lending portfolio away from high-emitting industries. 120 financial organisations have now signed up to the Net Zero Banking Alliance, covering over 40 percent of global banking assets, which commits members to work towards achieving net zero emissions from their lending and investment portfolio by 2050 or sooner.¹³

Engagement with financiers is particularly impactful within the request for lending phase, where directors should take care to ensure that ESG risks and exposures are appropriately managed. Failure to consider ESG risks and exposures within the organisation may lead to difficulties obtaining finance and debt investment in the future.

Directors can consider the following questions to develop a better understanding of financier's expectations:

- Do you understand the ESG concerns, expectations and data demands of banks and financial institutions?
- Do internal risk registers reflect these ESG concerns and expectations, and do you have risk mitigation and management processes in place for these concerns?
- How do you share and report your ESG risks and management to financiers? What ESG risk management processes do your financiers expect?
- How do you engage with financiers on ESG issues during the loan application and lending process?

¹³ KPMG Australia, 'Banking on the Climate Transition' (2023), <https://assets.kpmg.com/content/dam/kpmg/au/pdf/2023/banking-on-the-climate-transition.pdf>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

vii. Regulators and government – local, state, federal

Regulators and government bodies, though often grouped, may have different stakeholder priorities, and are in fact independent of each other. Regulators are specialised agencies, delegated with authority from the government to oversee laws, standards, and regulation within industries. Government on the other hand consists of elected officials, who represent the public and interests of their citizens. Therefore, their priorities are often dependent on political issues and vary within election cycles.

It is important for this reason to have separate approaches to engagement with these two stakeholders.

Regulators

The reputational and financial repercussions of regulatory scrutiny and action can be far-reaching. The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry¹⁴ provides a clear example of this, where intense regulatory scrutiny has had a significant impact on the reputation of large financial organisations.

Building a constructive and trusting relationship with regulators is, therefore, in the best interests of an organisation's shareholders or owners. Given the potential impact that mismanagement of regulatory stakeholders may have, directors are an increasingly critical part of an organisation's regulatory stakeholder engagement strategy.

Directors can have a bearing on this relationship in the following key ways:

Role of directors with respect to regulatory stakeholders	Questions to ask
Ensuring a clear understanding of the organisation's key regulators.	– What are the key regulators for the organisation/industry? – Do I understand the role and remit of each key regulator? – Am I familiar with each key regulator's objectives or stated focus areas (e.g. 'crackdowns' on certain areas of compliance)?
Understanding the key regulatory issues facing the organisation at any given time.	– If approached by a regulator, do I have the requisite knowledge and understanding of the key regulatory issues facing the organisation to adequately respond? – Am I satisfied with management's reporting of regulatory issues? – Do I know who the key relationship managers are within the organisation for each key regulator?
Setting and maintaining a culture of compliance throughout the organisation.	– Am I familiar with the measures in place to manage compliance issues throughout the organisation? – Have directors or management recently interacted with frontline staff to understand the prevailing attitude towards compliance? – Do employee engagement surveys highlight any cultural issues?
Establishing and demonstrating requirements for clear, open, transparent, and truthful communications with regulators.	– Am I role-modelling the behaviour I would expect from employees in my interactions and communications with regulators? – Have I witnessed (and corrected) any undesired behaviour or attitudes towards regulators?

¹⁴ Royal Commission, 'Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry', <https://www.royalcommission.gov.au/banking>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Government

Priorities of elected officials change between election cycles, for example based on majority party values and beliefs. It is important for directors to understand the political priorities, values and beliefs of majority parties and prepare for upcoming likely political changes leading into election periods.

Directors may develop stakeholder relations with government by:

- engaging via industry bodies and representatives
- developing a clear understanding of priorities for elected officials and the influence of these priorities on the organisation. See [Chapter 3](#) for more information on government entities.

viii. Civil society, multi-stakeholder bodies and NGOs

Engaging with civil society bodies, multi-stakeholder bodies and NGOs, including industry bodies and environmental and human rights advocacy groups (also called defenders) provides opportunities for boards to understand the interests, values and needs of their stakeholders through representative bodies, and to engage (and potentially collaborate) with them on these interests. This may be particularly useful and practical when, for example, the stakeholder group is large and/or dispersed, may not have the resources to take part in engagement opportunities, or is at risk of experiencing stakeholder fatigue.

Internationally, examples highlight the opportunity and imperative to engage with representative bodies. The 2024 EU Corporate Sustainability Due Diligence Directive, for example, which establishes a corporate due diligence duty that requires large companies to identify and address human rights and environmental impacts, requires that companies engage with their stakeholders either directly or via industry and multi-stakeholder initiatives. The United Nations Guiding Principles advises that organisations should also seek to identify their salient human rights issues, considering the perspectives of not just impacted stakeholders, but also those of expert stakeholders such as NGOs. This ensures that salient human rights issues are not overlooked.¹⁵

¹⁵ United Nations Guiding Principles reporting framework, 2017, Salient Human Rights Issues. Available at: [Salient Human Rights Issues : UN Guiding Principles Reporting Framework \(ungpreporting.org\)](https://www.un.org/ruhr/framework)

Engaging with civil society bodies, multi-stakeholder bodies and NGOs, including industry bodies and environmental and human rights advocacy groups may occur reactively, i.e. to respond to a concern or identified risk (seen most strikingly in response to protest), or can be undertaken proactively, seeking to identify opportunities for collaboration and partnership – this may be particularly important where there is an industry or sector-wide issue or risk to be addressed that can't be resolved effectively by working alone. Whatever approach is taken, engagement should be underpinned by respect. The United Nations Guiding Principles, for example, specifies in its commentary that the 'legitimate and peaceful activities of human rights defenders are not obstructed'.¹⁶

Engaging effectively with civil society bodies, multi-stakeholder bodies and NGOs can lead to better outcomes for all through managing risks to people and the community, while ineffective engagement can lead to the following negative consequences for organisations:

- Reputational damage or financial consequences for the organisation, including the potential for negative media coverage and delays in project approvals due to lack of social licence.
- Challenges in maintaining productive relationships with other stakeholders including elected representatives, which can lead to policy changes or outcomes that are contrary to the organisation's interests, for example, if a lack of voluntary action leads to action by regulators or legislators.
- Advocacy campaigns directed against the organisation and its activities.

Directors seeking to engage with civil society bodies, multi-stakeholder bodies and NGOs can begin by asking questions such as:

- Who are the key civil society bodies, multi-stakeholder bodies and NGOs that are interested in the organisation's activities and what are their interests and their level of influence? Who are the key individuals and who do they represent?
- How does the organisation currently engage with these stakeholders? Are there opportunities to engage more collaboratively?

¹⁶ United Nations, Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, p.29. Available at: [guidingprinciplesbusinesshr_en.pdf](https://www.un.org/ruhr/framework)

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ix. Media

Media organisations significantly shape awareness and perceptions of a business. Managing media is a proactive exercise that involves developing relationships with journalists so that a business can ensure coverage of its side of the story, especially at key moments. As senior representatives of a business, often with influence and – in the case of non-executive directors – some distance from the day-to-day, directors can play a meaningful role in engaging with media. Better-practice steps around engagement with media by businesses include:

- Mapping the publications and journalists who are interested in and influential over the mainstream media about relevant industry spaces.
- Developing a strategy and engagement plan for media.
- Developing strong, positive relationships with journalists who are authorities in these spaces.
- Providing clear position statements and relevant data on public-facing channels such as the company website and social media channels. These statements should be delivered consistently over time and across channels.
- Having a clear crisis management plan in place so that the business can convene, form solutions and act swiftly in a crisis.
- Monitoring media and social media to keep across the comments made about the business and its key people, so that the business can learn the likely issues and triggers for media attention and that any incorrect information can be corrected or otherwise addressed as necessary.
- Having in place PR consultants or agencies who can assist the business with expert advice, especially at stressful moments.

Engaging with the media using a disciplined, consistent approach can yield long-term benefits to:

- **The reputation of the business.** Positive media coverage can enhance a company's reputation, while negative coverage can damage it. Effective engagement with the media helps businesses maintain a positive image and manage crises.
- **The market positioning of the business.** Media exposure can help position a company as a leader in its industry. By highlighting innovations, achievements and contributions, businesses can differentiate themselves from competitors and attract customers and investors.
- **The policy or regulatory landscape for the business.** Businesses can use media to advocate for industry positions, influence public policy, and contribute to public discourse on relevant issues. This can enhance the company's influence and standing within its industry.
- **Crisis management in moments of mainstream criticism.** Media can help manage and mitigate potential damage to the company's reputation, or conversely can further harm it. Strong crisis management outcomes ensure that the company's perspective is accurately represented and helps control the narrative.

By strategically managing media relations, businesses can leverage media platforms to support their objectives, enhance their reputation, and build stronger relationships with key stakeholders.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

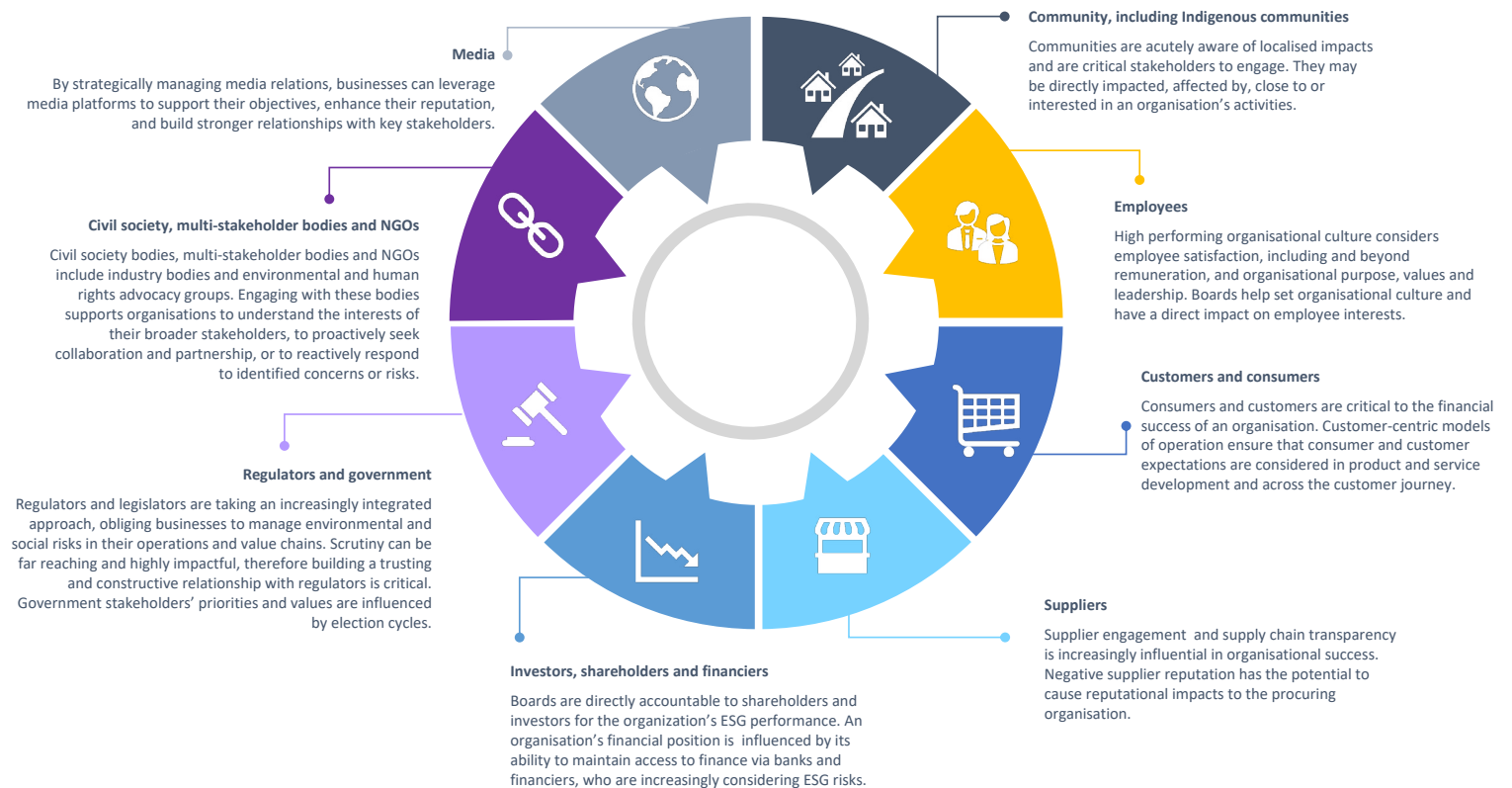


Figure 1 – Summary of the types of issues of relevance to stakeholders common to most organisations

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

• GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- AccountAbility 'AA1000 Stakeholder Engagement Standard' (2015), <https://www.accountability.org/standards/aa1000-stakeholder-engagement-standard/>
- Australian Institute of Company Directors (AICD), 'Dealing with regulator and other stakeholders – whose job is it anyway?' *Stakeholder Engagement* (Webpage, 13 June 2018), <https://aicd.companydirectors.com.au/membership/the-boardroom-report/volume-16-issue-6/dealing-with-the-regulator-and-other-stakeholders-whose-job-is-it-anyway>
- Zollinger. P., 2009, Stakeholder Engagement and the Board: Integrating Best Governance Practices – Global Corporate Governance Forum, <https://documents1.worldbank.org/curated/en/791711468330347261/pdf/629800WP0Stake00Box0361496B0PUBLIC0.pdf>

For further information please contact:



Louise Pogmore
Partner, Customer Advisory
KPMG Australia
lpogmore@kpmg.com.au



Dr Andy Symington
Director, ESG Social
KPMG Australia
asymington@kpmg.com.au

Governance Leadership

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

9. Structuring an Effective Board

Whether it be starting a new company or changing organisational structures, structuring an effective board is a challenging undertaking. The structure, composition, and internal dynamics of boards can affect the performance of individuals and the board collectively.

In this chapter

- Governance framework
- Code of conduct
- Skills and expertise
- Boardroom diversity
- Board size
- Getting the balance right
- Finding and appointing new directors
- Appointment process
- Director induction
- Director professional development
- The first 100 days
- Board evaluation
- Director remuneration
- Listed companies remuneration
- Re-election and rotation of directors
- Board succession planning
- Director tenure
- Access to company records

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

On establishment ...

1. Is there a structured plan, with timeframes and accountabilities, on how to establish the board?
2. Has an appointment letter setting out key terms and expectations been developed?
3. Has thought been given to appropriate remuneration arrangements (if any)?

Generally ...

4. Is the board considering its frameworks for communication with stakeholders in the first 100 days?
5. Are candidates/current directors able to commit sufficient time to discharge board duties?
6. Is there an appropriate induction program (including committee induction) for new directors?
7. Are the directors sufficiently familiar with the company's operations, performance, values and aspirations?
8. Is there a nomination committee charged with the responsibility of director succession planning, or alternatively, does the board have a robust process to enable orderly board succession?

9. Has the board adequately considered its approach to diversity including, where appropriate, the formulation of relevant policies?
10. Beyond having the right mix of skills, experience and background present on the board, does the composition complement the culture, engagement and style of the board?
11. Is a contingency plan established in the event that the chair has to step down unexpectedly?
12. Has the board properly considered the overarching strategy of the organisation and taken account of changes that are likely to occur in the short to medium term (for example changes to strategy, changes in the external environment) when determining its desired size and mix of skills/experience/backgrounds?
13. To the extent there are gaps in desired skills and experience that reside on the board, has the board adequately considered whether and how the board might benefit from the professional development of current board members?
14. Is the board setting the right tone and culture from the top and monitoring this?
15. Does the board regularly review its own performance and the effectiveness of its governance processes?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- On establishment – no advice is sought from experts or directors who have experience in establishing a new board.
- Not everyone agrees on the priorities and what is required from the board (at establishment phase and ongoing).
- The board comprises mainly inexperienced directors and limited induction programs are in place.
- Accountabilities and delegations are unclear and undocumented.
- No board instruments have been presented for endorsement (at establishment) or for review (ongoing).
- The board is too large or small compared with similar organisations.
- The board does not periodically review its skills and competencies or align its skills matrix to the company strategy.
- Board appointments are decided by the chair with little input from other directors.
- Limited or no consideration is given to the diversity of the board in its structure/composition and thought-process/decision-making processes.
- No consideration is given to the composition of, delegation to and reporting from board committees.
- Directors do not receive a letter setting out the terms and conditions of their appointment.
- No formal board induction is provided to new board members or this is insufficient.
- Board discussions are dominated by a small cohort of directors.
- The board finds it difficult to make decisions with consistent carryover of agenda items from one meeting to the next.
- Directors appear to be over-stretched and unable to dedicate sufficient time to their roles.
- Overuse of external advisers occurs due to skill gaps on the board.
- Directors are not provided with, or fail to engage with, professional development opportunities.
- There is no board evaluation/review process (or it is not documented or known to the board).
- There is a failure to appreciate the implications of the two-strike rule on the remuneration report or to anticipate members' reaction to the remuneration report.
- No consideration is given to the enforcement of accountability for non-remunerated directors.
- There is a lack of ongoing board succession planning.
- Directors have difficulty accessing company information in a timely manner.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

GOVERNANCE FRAMEWORK

Effective boards are boards that are able to consistently and constructively make proactive decisions that ensure the sustainable success of their organisation. Effective board composition is the bedrock of an effective board, helping to limit the potential for board complacency criticised in the APRA CBA report.¹ ASX Corporate Governance Principles and Recommendations Principle 2 commentary states that 'a high performing, effective board is essential for the proper governance of a listed entity.'²

In practice, the company's governance embodies a complex range of structures (frameworks, policies, and processes) balanced against the appropriate mix of skills, behaviours, and practices.

A well-designed governance framework will help the board to be effective and fulfil its role by:

- instilling the desired behaviours that underpin the company's core values and drive the cultural 'tone from the top'
- giving an audience to 'the customer voice' and the voice of other key stakeholders
- instilling confidence in shareholders and the public that the company is well-governed
- ensuring that directors' competencies and skills are appropriate given the company's current and future strategic requirements
- empowering the board to act to its best capability by having the appropriate mix of skills, expertise, experience and diversity of thought
- clarifying the roles, responsibilities and delegation of powers of individual directors, the board, its committees, and management
- matching the skills and expertise of individual directors with board and committee responsibilities

- ensuring that directors have access to an induction program and ongoing professional development
- implementing sound risk management practices and controls in line with the organisation's risk appetite
- facilitating the evaluation and review of the board, chair, CEO, and management
- embedding processes that facilitate the board's oversight and constructive challenge of management
- including transparent mechanisms for the enforcement of accountability by the board and management
- aligning the remuneration strategy with the shareholders' expectations, rather than encouraging short-term profits and self-interest, thereby safeguarding the shareholders' interests
- enabling the efficient and effective reporting of quality information on a timely basis between directors, the board and its committees, the company executives, the organisation as a whole, and wider stakeholders.

Recommendation 2.1 of the ASX Corporate Governance Principles and Recommendations suggests that the board of a listed entity have a separate nomination committee (comprising of a majority of independent directors), as it can be 'an efficient and effective mechanism to bring the transparency, focus and independent judgement needed to decisions regarding the composition of the board'. The nomination committee should have a charter which 'clearly sets out its role and confers on it all necessary powers to perform that role. This will usually include the right to seek advice from external consultants or specialists where the committee considers that necessary or appropriate'. If the company does not have a nomination committee, then the entity should 'disclose that fact and the processes it employs to address board succession issues and ensure that the board has the appropriate balance of skills, knowledge, experience, independence and diversity to enable it to discharge its duties and responsibilities effectively.' Further information on committees can be found in [Chapter 11](#).

¹ APRA Prudential Inquiry into The Commonwealth Bank of Australia report (April 2018), https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf

² ASX Corporate Governance Principles and Recommendations (4th edition).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Governance practices came under the spotlight following the Hayne Royal Commission and have stayed there since. In 2018 ASIC introduced the Corporate Governance Taskforce. This taskforce was established to undertake targeted reviews of corporate governance practices in large listed entities and to 'allow ASIC to shine a light on 'good' and 'bad' practices observed across these entities'.³ The first report produced by this Taskforce in October 2019 addresses ASIC's observations on director and officer oversight of non-financial risk in large and complex financial services companies.⁴ In summary, the following findings are contained within the report:

- All too often, management was operating outside of board-approved risk appetites for non-financial risks, particularly compliance risk. Boards need to actively hold management accountable for operating within stated risk appetites.
- Reporting of risk against appetite often did not effectively communicate the company's risk position. Boards need to take ownership of the form and content of information they are receiving so that they can adequately oversee the management of material risks.
- Material information about non-financial risk was often buried in dense, voluminous board packs. It was difficult to identify key non-financial risk issues in information presented to the board. Boards should require reporting from management that has a clear hierarchy and prioritisation of non-financial risks.
- The effectiveness of board risk committees (BRCs) could be improved. BRCs should meet more regularly, devote enough time and be actively engaged to oversee material risks in a timely and effective manner.⁵

ASIC Chair, James Shipton, made the following statements in the accompanying media statement.

- 3 ASIC, 2018, An ASIC update by John Price, Commissioner, <https://asic.gov.au/about-asic/news-centre/speeches/an-asic-update-by-john-price-commissioner/>
- 4 ASIC, Corporate Governance Taskforce, Director and officer oversight of non-financial risk report, <https://asic.gov.au/regulatory-resources/find-a-document/reports/corporate-governance-taskforce-director-and-officer-oversight-of-non-financial-risk-report/>
- 5 ASIC, 2019, ASIC releases report on director and officer oversight of non-financial risk, <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2019-releases/19-271mr-asic-releases-report-on-director-and-officer-oversight-of-non-financial-risk/>

'While there is no 'one-size-fits-all' solution to these findings, boards need to proactively identify and assess their own characteristics and processes. Though the review examined companies in the financial services industry, many of the lessons learned can be applied to most public companies in other sectors of the economy.'

*'Our report concludes with a series of questions that all public companies might ask themselves. Not all will be relevant to every company, but many will be. We urge boards of all large listed companies to read this report and review their governance practices and accountability structures with reference to our findings.'*⁶

Based on the most recent Governance Review Report produced by APRA, more work is still required in this area. This report states that since 2018, APRA has accepted seven court-enforceable undertakings as well as imposed five capital overlays for insurers, seven capital overlays for banks, and thirteen occasions of additional licence conditions for RSE licensees which were all due to governance concerns.⁷

VALUES AND CODE OF CONDUCT

Recommendation 3.1 of the ASX Corporate Governance Principles and Recommendations states that 'a listed entity should articulate and disclose its values'. The recommendation commentary notes that 'a listed entity's values are the guiding principles and norms that define what type of organisation it aspires to be and what it requires from its directors, senior executives and employees to achieve that aspiration'. Flowing from there, Recommendation 3.2 suggests that boards of listed companies should have and disclose a code of conduct for its directors, senior executives, and employees that 'articulates the standards of behaviour expected from directors, senior executives and employees' and ensure that 'the board or a committee of the board should be informed of any material breaches of the entity's code of conduct as they may be indicative of issues with the culture of the organisation'.⁸

- 6 ASIC, 2019, ASIC releases report on director and officer oversight of non-financial risk, <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2019-releases/19-271mr-asic-releases-report-on-director-and-officer-oversight-of-non-financial-risk/>
- 7 APRA, March 2020, Governance Review Discussion Paper, <https://www.apra.gov.au/sites/default/files/2025-03/Governance%20Review%20-%20%20Discussion%20Paper.pdf>
- 8 Refer to Principle 3.2 of ASX Corporate Governance Principles and Recommendations (4th edition), <https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/cgc-principles-and-recommendations-fourth-edn.pdf>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The commentary for Recommendation 3.2 also includes a list of 'Suggestions for the content of a code of conduct' which is a useful point of reference.⁹ The board's role in setting and monitoring culture is further discussed in [Chapter 22](#).

SKILLS AND EXPERTISE

The board should collectively possess a sufficient range of competencies to effectively deal with the issues and opportunities the company faces. It should be comprised of individuals who bring to the boardroom a range of skills and know-how in relevant areas. Their individual strengths should complement each other.

The competencies required for any particular board will vary considerably, depending on the company's strategy, development stage and the industry and broader environment in which it operates. The types of generic technical skills and competencies required on a board might include:

- accounting and finance
- business judgement
- industry knowledge
- government knowledge
- legal knowledge
- employment/industrial relations knowledge
- environment/sustainability knowledge
- leadership
- strategy/vision
- risk management.

⁹ Refer to Box 3.2: Suggestions for the content of a code of conduct of ASX Corporate Governance Principles and Recommendations (4th edition), <https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/cgc-principles-and-recommendations-fourth-edn.pdf>

With technological advancements and the risk of cyberattack being front of mind for boards, many boards are also looking for technology skills.

Similarly, given the increased focus on conduct risk and other non-financial risks as noted before, there is an increased focus on ensuring directors possess the appropriate behavioural competencies, as well as the traditional technical skills. Behavioural attributes include:

- emotional intelligence
- curiosity
- an appreciation for diversity of thought, backgrounds, expertise and experience
- authenticity
- transparency in decision-making and communication
- self-awareness and accountability
- willingness to reflect, learn and adapt
- ability to challenge and question in a constructive manner
- sense of rigour and ability to enforce accountability in an appropriate manner
- humility to know that they will not have all the answers.

Board skills matrix

Recommendation 2.2 of the ASX Corporate Governance Principles and Recommendations states that companies should have and disclose a 'board skills matrix' setting out the mix of capability and diversity that the board currently has, or is looking to achieve, in its membership.

The Recommendation commentary notes that there is no prescribed format for a board skills matrix. It can set out either the mix of skills that the board currently has or the mix of skills that the board is looking to achieve in its membership or both. Whichever format it follows, the listed company should explain what it means when it refers to a particular skill in its board skills matrix and the criteria a director must meet to be considered to have that skill.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

In addition to a technical competency assessment, the skills matrix should ideally also include an analysis of the current or desired behaviours to help the board function as an effective decision-making body.

The skills matrix is a useful tool to identify gaps in the collective board's skills (which should be addressed by appointing new members or providing professional development to existing directors) as well as succession planning.

Disclosing the board skills matrix also 'gives useful information to investors and helps to increase the accountability of the board in ensuring it has the skills to discharge its obligations effectively and to add value'.¹⁰

BOARDROOM DIVERSITY

The ASX Corporate Governance Principles and Recommendations describe various facets of diversity being gender, age, ethnicity and background which 'can help bring different perspectives and experiences to bear and avoid 'groupthink' or other cognitive biases in decision making'.¹¹

The economic arguments for more board diversity have been identified in various widely publicised studies. These studies demonstrate a correlation between increased diversity at higher levels of the organisation and stronger organisational and financial performance.¹²

¹⁰ Refer to commentary for Recommendation 2.2 of ASX Corporate Governance Principles and Recommendations (4th edition)

¹¹ Refer to commentary for Recommendation 1.5 of ASX Corporate Governance Principles and Recommendations (4th edition)

¹² See for example – Gender Diversity and Corporate Performance, Credit Suisse Research Institute, August 2012; The Bottom Line: Corporate Performance and Women's Representation on boards, Catalyst, October 2007; Australia's Hidden Resource: The economic case for increasing female participation, Goldman Sachs JB Were, November 2009.

In structuring the board to add value from diversity, a company should consider the mix of skills, backgrounds, experience, expertise, age, gender and perspectives of its directors that would be necessary to meet the unique requirements of the company. An emphasis on director diversity should yield a number of key benefits:

- an increase in the intellectual resources of the board and reduction in the reliance on the authority of key individuals
- derive value from previously unrecognised or overlooked opportunities
- enhancement of the board's ability for reflection and decision-making capabilities, thus lessening the risk of 'groupthink', 'dulling of the senses' or the 'chronic ease' criticised in the APRA CBA report
- a stronger sense of board authenticity and connection with customers, employees and other stakeholders, helping to set the cultural 'tone from the top' and critical to the company's 'social licence to operate'
- improving skills to constructively challenge and hold management to account, reducing the chance of overconfidence in management and the company's performance as a whole, particularly with regard to risk management.

To encourage companies to foster a governance culture that embraces diversity, Recommendation 1.5 of the ASX Corporate Governance Principles and Recommendations requires listed entities to:

- have and disclose a diversity policy (and Box 1.5: *Suggestions for the content of a diversity policy*¹³ in the commentary may prove helpful in formulating or updating diversity policy)
- set measurable objectives for achieving gender diversity in the composition of the board, senior executives and the workforce generally
- charge management with designing, implementing and maintaining programs and initiatives to help achieve those measurable objectives

¹³ Refer to commentary for Recommendation 1.5 of the ASX Corporate Governance Principles and Recommendations (4th edition).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

- review with management and disclose at least annually:
 - the measurable objectives set by the board, particularly for achieving gender diversity
 - the progress towards achieving those measurable objectives
 - the adequacy of the entity's programs and initiatives in that regard
 - whether the review referred to above has taken place
 - note the respective proportions of men and women on the board, in senior executive positions and across the whole workforce (or if the entity is a 'relevant employer' under the Workplace Gender Equality Act, the entity's most recent 'Gender Equality Indicators', as defined in and published under that Act).¹⁴

If the entity was in the S&P/ASX 300 index at the commencement of the reporting period, the measurable objective for achieving gender diversity in the composition of its board should be to have not less than 30 percent of its directors of each gender within a specified period.

The ASX recommendations specific focus on gender diversity is supported by reference to Bankwest Curtin Economics Centre's 2020 report 'More women at the top proves better for business', which observes that an increase of 10 percentage points or more in female representation on the boards of Australian ASX-listed companies led to a 4.9 percent increase in the company market value. These companies also had a 12.9 percent increase in the likelihood of outperforming the sector on three or more performance and profitability metrics.¹⁵

Interestingly, a more recent report from the same Centre describes a causal link between increased female board representation and lower incidence of corporate fraud suggesting that potentially governance and oversight are improved where a more diverse board is in place.¹⁶

¹⁴ Recommendation 1.5(c) of the ASX Corporate Governance Principles and Recommendations (4th edition).

¹⁵ Bankwest Curtin Economics Centre, 'More women at the top proves better for business', <https://bcec.edu.au/media/more-women-at-the-top-proves-better-for-business/>

¹⁶ Bankwest Curtin Economics Centre, *Women in the Boardroom and Fraud: Evidence from Australia* <https://bcec.edu.au/publications/women-in-the-boardroom-and-fraud-evidence-from-australia/>

The Australian Institute of Company Directors (AICD) tracks new board appointments on a quarterly basis. They report that as at 30 June 2025, the percentage of women on boards of ASX 200 companies was 38.1% (up from 34.2% when we last published this toolkit in 2022 and provided the November 2021 statistics),¹⁷ with companies in the ASX 50 and ASX 20 having exceeded the 40% threshold, at 41% and 42% respectively and no boards in the ASX 200 without women.¹⁸ Further, this report identifies that 25 boards in the ASX 200 have female chairs.

The major proxy advisors in Australia disclose in their Proxy Voting Guidelines for 2025 their expectations regarding diversity however this is currently limited to gender diversity only (see for example Glass Lewis¹⁹ and ISS²⁰). In the United Kingdom these expectations are broader reaching and Glass Lewis has declared in their 2025 Corporate Governance Policy Guidelines for the UK that 'from 2025, Glass Lewis' benchmark policy will generally recommend against the re-election of the chair of the nomination committee at any FTSE 250 board that has failed to appoint at least one director from an ethnic minority background and has failed to provide a clear and compelling rationale for the lack of board-level ethnic diversity'.²¹

Recommendation 9.1 of the ASX Corporate Governance Principles and Recommendations requires a listed entity to disclose the processes it has in place to ensure that its directors of a different primary language (to that of the other directors and the language used in key documents) understand and can contribute to the discussions at board meetings and understand and can discharge their obligations in relation to key documents. This highlights the challenges that diversity can entail and how processes are required to ensure that inclusion is achieved as well as diversity.

¹⁷ Bankwest Curtin Economics Centre, *Women in the Boardroom and Fraud: Evidence from Australia* <https://bcec.edu.au/publications/women-in-the-boardroom-and-fraud-evidence-from-australia/>

¹⁸ AICD, Women on ASX 200 Boards (at 30 November 2021) <http://aicd.companydirectors.com.au/advocacy/board-diversity/statistics>

¹⁹ <https://resources.glasslewis.com/hubfs/2025%20Guidelines/Australia%202025%20Benchmark%20Policy%20Guidelines.pdf>

²⁰ <https://www.issgovernance.com/file/policy/active/asiapacific/Australia-Voting-Guidelines.pdf?v=1>

²¹ CGI Glass Lewis 2025 Policy Guidelines (United Kingdom),

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Diversity is a key cornerstone to a dynamic, effective board. A board should be able to illicit the skills required to adapt, embrace change, co-operate with key stakeholders to proactively respond to challenges, identify and exploit opportunities, harness its social licence to operate and build long-term sustainable success. Boards and directors that fail to embrace diversity (in all its forms) will become less relevant and influential which is likely one of the drivers for the broader diversity requirements described by proxy advisors in jurisdictions like the UK as discussed before.

BOARD SIZE

The Corporations Act specifies that public company boards should have a minimum of three directors.²² ASX Corporate Governance Principles and Recommendations Principle 2 states that 'a listed entity should have a board of an appropriate size, composition, skills, commitment and knowledge of the entity and the industry in which it operates, to enable it to discharge its duties effectively and to add value' and that the board 'should be of sufficient size so that the requirements of the business can be met and changes to the composition of the board and its committees can be managed without undue disruption. However, it should not be so large as to be unwieldy'.

In practice, the optimum size for any particular board will reflect several factors, including the:

- size and complexity of the company and its operations
- range of competencies and behavioural skills needed to handle the evolving circumstances and needs of the board and company as a whole
- need, if required, to achieve an appropriate mix of executive and non-executive directors
- need, if required, to allow for the appointment of nominee directors by institutional investors
- number and nature of board committees (audit committee, nomination committee, etc.)
- need to raise a quorum.

²² Corporations Act 2001, Section 201A(2).

FINDING AND APPOINTING NEW DIRECTORS

Recommendation 2.1 of the ASX Corporate Governance Principles and Recommendations suggests that 'to promote investor confidence, there should be a formal, rigorous and transparent process for the appointment and reappointment of directors to the board'.

The recommendation commentary states that 'the process for recruiting a new director, including evaluating the balance of skills, knowledge, experience, independence and diversity on the board and, in the light of this evaluation, preparing a description of the role and capabilities required for a particular appointment' is part of the role of the nomination committee. When searching for a new director, the nomination committee should thoroughly review the existing board's strengths and weaknesses, skills and experience gaps, current age range and gender composition, and its ambitions for the future. The outcome of this process will be a brief containing detailed selection criteria approved by the board. There are numerous organisations that can assist with independent board skills assessments, as well as a range of tools and templates designed to provide guidance on better practice approaches.²³ All boards should adopt a proactive, systematic and transparent approach to board appointments, and develop a succession plan. The nomination committee should have specific responsibility for identifying suitable candidates, working at least 9–12 months ahead of anticipated board vacancies.

The Corporations Act imposes no educational or specific qualification requirements for directors, although the following people are excluded from holding office as a director:

- an undischarged bankrupt cannot act as a company director, or participate in the management of a company without the permission of a court²⁴

²³ Examples include Governance Institute of Australia <https://www.governanceinstitute.com.au> and Australian Institute of Company Directors <https://aicd.companydirectors.com.au>

²⁴ Corporations Act 2001, Sections 206B(3) and 206G.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

- anyone convicted of certain offences cannot act as a director within five years of their conviction or release from prison, without the permission of a court²⁵
- anybody disqualified from managing a company as a result of a court order.

Depending on the industry in which a company operates, there may be other regulatory requirements relevant to director appointments emanating from sources other than the Corporations Act. For example, corporations regulated by APRA need to ensure compliance with CPS 510 Governance and CPS 510 Fit and Proper. Government entities are subject to different appointment processes (including candidate selection), which are outlined in the entity's Enabling Act.

The ASX Listing Rules require that entities which are applying for listing to satisfy the ASX that each director or proposed director, the CEO or proposed CEO (if the CEO is not a director) and the CFO or proposed CFO, is of 'good fame and character'.²⁶ Whilst this is a formal requirement that applies to companies that are seeking to be listed, the 'good fame and character' requirement is something that all companies should consider when appointing new directors.

Individuals are required to have a Director Identification Number (ID) if they are a director or an alternate director who is acting in that capacity ('an eligible officer') of:

- a company, a *registered* Australian body or a registered foreign company under the *Corporations Act 2001* (Corporations Act)
- an Aboriginal and Torres Strait Islander corporation registered under the *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (CATSI Act).²⁷

²⁵ Corporations Act 2001, Sections 206B(2) and 206G.

²⁶ ASX Listing Rule 1.1, Condition 20.

²⁷ ABRS, 2021, Who needs to apply and when, <https://www.abrs.gov.au/director-identification-number/who-needs-apply-and-when>

There are penalties for non-compliance such as fines or imprisonment for failing to apply or misusing a director ID. Further, applying for multiple IDs or misrepresenting an ID can result in up to one year imprisonment.²⁸

APPOINTMENT PROCESS

Initial appointment

There are some limitations on who can be appointed as a director. For example, an individual must be at least 18 years old. A person who is disqualified from managing companies can only be appointed as a director if the appointment is made with the permission granted by ASIC or leave granted by a court.²⁹

Directors are normally appointed by a resolution³⁰ passed by members at a general meeting of the company. Directors must provide a signed consent to act to the company prior to being appointed.³¹

Recommendation 1.2 of the ASX Corporate Governance Principles and Recommendations recommends that a listed entity should undertake appropriate checks before appointing a person or putting forward a candidate to security holders for election as a director, and provide security holders with all material information in its possession relevant to their decision to elect or re-elect a director (including a summary of information that should be provided to help security holders make an informed decision).³²

²⁸ <https://www.asic.gov.au/for-business-and-companies/companies/company-officeholder-rules-and-changes/director-identification-numbers-director-ids/#penalties-relating-to-director-ids>

²⁹ Corporations Act 2001, Section 201B.

³⁰ Refer to Corporations Act 2001, Section 201G for legislation regarding approval of Director appointment by members.

³¹ Corporations Act 2001, Section 201D.

³² Recommendation 1.2 of the ASX Corporate Governance Principles and Recommendations (4th edition).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

For new appointments, the board should provide the security holders with details of the candidate, including:

- biographical details, including relevant qualifications, experience and skills
- material directorships currently held by the candidate
- potential conflicts of interests and close personal ties that may influence the candidate's judgement.

These details are particularly relevant for proposed independent director appointments, and as such, require a statement by the board as to the whether it supports the election of the candidate and their rationale. The committee would also 'usually include checks as to the person's character, experience, education, criminal record and bankruptcy history'³³ and the provision of Director Identification Numbers does not remove this requirement to perform appropriate due diligence.

Depending upon the company's constitution, the existing directors may also be able to appoint directors usually to fill casual vacancies.³⁴ If appointed in this manner, public companies must confirm the appointment by resolution at the company's next AGM.³⁵ In the case of a proprietary company governed by the Replaceable Rules, the appointment must be confirmed by the company within two months of the time the appointment is made;³⁶ ASIC must be notified within 28 days of an appointment. Listed companies must comply with the relevant ASX Listing Rule requirements, (some of which may also be included in a company's constitution), which include, for instance, the requirement to hold director elections each year and director rotation requirements.³⁷

³³ *ibid.*

³⁴ Corporations Act 2001, Section 201H.

³⁵ Corporations Act 2001, Section 201H(3).

³⁶ Corporations Act 2001, Section 201H(2).

³⁷ See specifically ASX Listing Rules 14.3, 14.4 and 14.5.

Director letter of appointment

When a new director has consented to the appointment, they should receive a letter of appointment setting out the key terms and conditions of the appointment. The form of the agreement will differ depending on whether the director holds an executive or non-executive position. There are a number of guides³⁸ as to what should be included in appointment letters, although this will generally depend on the size, structure and individual circumstances of the company. Listing Rule 3.16.4 requires an entity to disclose the material terms of any employment or service contract (or any variation to it) with the CEO (or equivalent) and any of its directors. For a general guide of what should be included in a non-executive director or executive director (or other senior executive) agreement, refer to the ASX Corporate Governance Principles and Recommendations commentary to Recommendation 1.3.

Director due diligence

The role of the company director has become increasingly onerous and time-consuming with directors bearing increased responsibility and liability. It is critical for prospective directors to undertake their own due diligence on the companies they are invited to join, to ensure they can make a useful contribution and effectively discharge their duties.

Prior to accepting a board appointment, an individual should:

- investigate the particular company and the industry in which it operates
- gather information about the people in leadership roles and arrange to speak with key directors and senior management
- review documentation supplied by the company, such as company policies and strategy

³⁸ Refer to AICD guidelines on letter of appointment for Directors <https://www.aicd.com.au/board-of-directors/roles/appointment/letter-of-appointment.html>, ACNC guide on letter of appointment for responsible persons <https://www.acnc.gov.au/tools/templates/letter-appointment-for-responsible-people> and Governance Institute of Australia's 'Good Governance Guide — Letters of appointment for non-executive Directors: suggested contents' and 'Letter of Appointment' template available at <https://www.governanceinstitute.com.au/>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

- be satisfied that they are equipped with the requisite skills and knowledge to properly discharge the responsibilities of a director
- assess their ability to contribute the requisite technical and interpersonal skills to enable them to build effective working relationships with the rest of the board and the executive team.

Board members are encouraged to have a personal contingency plan to deal with the additional time constraints and commitment required during a particularly busy or challenging period for an entity, whilst balancing other work and personal commitments. Going one step further, directors should consider how they would handle an unanticipated surge in workload from other board roles.³⁹

The AICD's 'Director Tools: Board composition – evaluating an organisation before joining' is a useful point of further reference.⁴⁰

DIRECTOR INDUCTION

In light of the Hayne Royal Commission there should be a concerted focus on getting directors 'up to speed' as quickly as possible.⁴¹ The need to get new directors 'up to speed' as quickly as possible relates not only to directors' due diligence, but also to the induction provided by entities, as induction programs make it more likely that new directors can make an immediate contribution.

Director induction programs are designed to make the most out of a director's existing knowledge base by filling any knowledge gaps, typically concerning the company's industry, the competitive landscape and technical issues, as well as familiarising the director with all aspects of the company, including risk management. Increasingly, induction is also recognised as a key tool in a company's ethical framework, used to instil the desired cultural values and

behaviours of the organisation. Periodic and ongoing professional development aids the reinforcement of those values and principles.

There is no prescriptive formula for what should be included in an induction program. The elements of the program should be tailored to take account of the appointee's knowledge and experience, and will vary depending on company structure, processes and the major issues it faces.

Recommendation 2.6 of the ASX Corporate Governance Principles and Recommendations suggests that a company should have an induction program in place for new directors. Recommendations 1.4 and 2.1 of the ASX Corporate Governance Principles and Recommendations suggest that it is the responsibility of the company secretary and the nomination committee to organise and facilitate the induction and professional development of directors.⁴² An induction program for a new director may include the following:

- *Corporate information* – mission statement, values and code of conduct, strategic and business plans, financial accounts, legal and regulatory frameworks, major shareholders, corporate communications, overview of the company's competitors and industry information, risk profile and appetite, company history and product information.
- *Governance framework* – board charter/governance statement, annual agenda, selected board packs, full details of directors, committee structures, board process, assurance providers, resources available, key stakeholders, procedures for sign-off of financial statements and items requiring approval outside of board meetings.
- *Management information* – names and background of senior management, organisational and management structure outline, etc.

³⁹ Refer to AICD, 2018, Final round of Royal Commission hearings, <https://aicd.companydirectors.com.au/membership/membership-update/final-round-of-royal-commission-hearings>

⁴⁰ AICD, Evaluating an organisation before joining, <http://aicd.companydirectors.com.au/-/media/cd2/resources/director-resources/director-tools/2019/individual/07236-5-1-evaluating-an-organisation-before-joining-fa.ashx>

⁴¹ Refer to AICD, 2018, Final round of Royal Commission hearings, <https://aicd.companydirectors.com.au/membership/membership-update/final-round-of-royal-commission-hearings>

⁴² Recommendations 1.4 and 2.1 of the ASX Corporate Governance Principles and Recommendations (4th edition).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

- *Legal and accounting training* – if a new director is not familiar with the legal framework that governs the entity and/or if the director does not have accounting skills or knowledge.
- *Technology training* – to optimise the use of dashboards and other technology in the boardroom. Technology training at the induction stage may also facilitate the directors' adoption of new technology in the future.⁴³

Both the AICD and Institute of Community Directors provide free guidance on their website regarding the typical matters covered in an induction pack.⁴⁴

Typically, a combination of written materials, coupled with presentations and activities, such as meetings and site visits, will provide the appointee with a realistic picture of the company's position and the challenges it faces. It will also serve to foster a constructive relationship between the new director and their fellow directors and senior management. In addition to the provision of induction materials, it is also important to schedule interviews with key senior executives to gain an understanding of the entity's structure, business operations, history, culture, and key risks.⁴⁵

An induction to board committees, with particular emphasis on those board committees which the new director will join, should not be overlooked. An induction pack containing relevant documents such as committee charters, annual agendas, copies of minutes, plus a full briefing by the relevant committee chair will help the new director gain an appreciation of the major issues.

⁴³ Refer to Recommendation 2.6 of the ASX Corporate Governance Principles and Recommendations (4th edition)

⁴⁴ Refer to Institute of Community Directors <https://communitydirectors.com.au/check-lists/checklist-for-an-effective-induction>

⁴⁵ Refer to commentary for Recommendation 2.6 of the ASX Corporate Governance Principles and Recommendations (4th edition).

DIRECTOR PROFESSIONAL DEVELOPMENT

As well as providing induction programs for new directors, boards should also encourage and finance continuing director education.

Through the board evaluation process, areas will be identified where further education may enhance board and individual director effectiveness. The board should ensure that resources are budgeted to provide appropriate educational opportunities for directors. The chair should address the developmental needs of the board as a whole, plus those of individual directors, with the company secretary playing a key role in facilitating the process.

The commentary for Recommendation 2.6 of the ASX Corporate Governance Principles and Recommendations recommends that professional development for directors should be considered where gaps are identified and they are not expected to be addressed in the short term by new appointments.⁴⁶ The commentary further notes that 'the board or nomination committee should ensure that directors receive briefings on material developments in laws, regulations and accounting standards relevant to the entity'. As the need to interpret and critique non-financial reports becomes increasingly relevant, boards would also be wise to broaden the scope of such briefings and director training programs to include integrated reporting. The development of behavioural skills to help embed the cultural 'tone from the top' is also likely to become increasingly important.

Professional development requires an ongoing commitment from individual directors to continually reflect, learn, challenge and adapt. Directors with long tenures can often feel that they know the business and their role well enough to not require ongoing education, however, the reverse is often the case. Such complacency is a key component of the 'chronic ease' and over-reliance on key individuals repeatedly criticised of CBA in the APRA CBA report.⁴⁷ Complacency and overconfidence can quickly make directors – and their organisations – irrelevant. Directors who do not value and engage in professional development are red flags for any board.

⁴⁶ Recommendation 2.6 of the ASX Corporate Governance Principles and Recommendations (4th edition).

⁴⁷ Refer to the Executive Summary, Sections 2.2.2, 2.2.3, 9.2.6 and 9.2.7 and of APRA Prudential Inquiry into The Commonwealth Bank of Australia report (April 2018) https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

THE FIRST 100 DAYS FRAMEWORK

Directors appointed to newly formed boards are required to oversee the challenging task of establishing a functioning boardroom and effective corporate governance structure. The first 100 days framework provides a high-level roadmap of the key activities and deliverables needed to establish an effective board within a target timeframe of 100 days. It can be applied for new boards or used as a checklist for existing boards.

The framework begins by establishing a direction and clear set of priorities for the newly established board. During this stage, the board should document its plan, and establish timelines and accountabilities around achieving its milestones.

Importantly, the board should then consider its risk management – setting its overall 'risk appetite' and documenting what it considers are the critical risks facing the organisation. With these considerations in mind, the board should then define its target operating model, appoint its key management personnel and endorse policies to guide the organisation.

While this is occurring, the board should be engaging shareholders and key stakeholders and overseeing the development of an accountability and compliance framework.

First 100 days framework

Governance priorities	Risk profile	Operating model	Stakeholder framework	Compliance
– Terms of reference – Charter and annual agenda – Subcommittees – Financial compliance – Legal and compliance duties – Retained authorities – Delegations/CEO limits – Code of conduct – Strategic plan	– Risk management policy – Risk workshop – Agree and validate critical risks – Risk register – Risk monitoring and mitigation – Risk reporting framework	– Policies: – Conflicts of interest – Regulatory compliance – Privacy – Whistleblower & Fraud – Media/crisis/incident – Continuous disclosure – Target operating model – Key appointments CEO/CFO	– Communication policy – Internal/shareholders/community/government – Shareholder relations – Mapping & tiering – Engagement plan – Consultation model – Shareholder and consumer participation forums	– Compliance framework – Internal and external auditor appointment – Audit and risk committee – Consequence and breach policy – Reporting & oversight – Board performance assessments
Leadership & strategy	Risk management	Performance & monitoring	Stakeholder engagement	Accountability & audit
<i>Informed discussions and decisions, not an endless stream of surprises.</i>	<i>Proactive, strategic tool, not a reactive function.</i>	<i>Healthy culture supported by strong policies, not an inconsistent 'tone at the top'.</i>	<i>Active stakeholder consultation, not disengagement from the process.</i>	<i>Tailored assurance and reporting, not a 'one size fits all' approach.</i>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

BOARD EVALUATION

As previously stated in the 'Finding and appointing new directors' section of this chapter, Recommendation 2.1 of the ASX Corporate Governance Principles and Recommendations states that 'to promote investor confidence, there should be a formal, rigorous and transparent process for the appointment and reappointment of directors to the board.' The reappointment of directors is inextricably linked to the evaluation of the board.

Board evaluation is also a useful process in identifying the critical success factors for improving the effectiveness and efficiency of the board and its committees. It encourages directors to examine their own contribution and, when expertly facilitated, can improve working relationships between directors.

Recommendation 1.6 of the ASX Corporate Governance Principles and Recommendations recommends that a listed entity should have, and disclose, a process for periodically evaluating the performance of the board, its committees and individual directors, and should disclose whether the performance evaluation was undertaken in accordance with that process during the reporting period.⁴⁸ Other standards, including Australian Standards Good Governance Principles AS 8000-2003 and Prudential Standard CPS 510 Governance include similar recommendations.

The commentary for Recommendation 2.1 of the ASX Corporate Governance Principles and Recommendations suggests that the nomination committee should consider implementing a plan for evaluating the balance of skills, knowledge, experience, independence and diversity on the board. The rationale for this approach is that such an evaluation will enable the identification of specific skills that will best increase board effectiveness.

The commentary for Recommendation 2.6 of the ASX Corporate Governance Principles and Recommendations also notes that the board or nomination committee should regularly assess/evaluate whether the directors as a group have the skills, knowledge and experience to deal with new and emerging business and governance issues. These may include cyber security, AI and data analytics, climate change, conduct and culture related matters.

⁴⁸ Recommendation 1.6 of the ASX Corporate Governance Principles and Recommendations (4th edition).

Evaluation of non-executive directors and the chairperson

Principle 2 of the ASX Corporate Governance Principles and Recommendations emphasises the importance of the board's ability to evaluate the independence of its independent directors. Recommendations 2.3 and 2.4 focus specifically on independent directors. The wording of 'Box 2.3 – Factors relevant to assessing the independence of a director' of the ASX Corporate Governance Principles and Recommendations has seen a number of amendments since the 3rd edition to simplify the wording and expand the factors for consideration when evaluating a director's independence and is a useful point of reference.⁴⁹

The commentary for Recommendation 2.1 also suggests that the board or nomination committee should 'regularly review the time required from a non-executive director and whether directors are meeting that requirement'.⁵⁰ The time committed by directors was also one of the governance-related issues highlighted during the Hayne Royal Commission. It may be argued that the increasing demands of governing large and complex corporates has resulted in the need for non-executive directors to dedicate more time to their roles, in order to sufficiently discharge their duties. The impact of COVID-19 on boards who met more regularly, especially in the initial stages of the pandemic, highlighted that directors need capacity to deal with multiple crises across multiple companies simultaneously. To this end, there has been an increased focus on director capacity and 'overboarding' globally, for example:

- The UK Corporate Governance Code (January 2024) states that 'When making new appointments, the board should take into account other demands on directors' time. Prior to appointment, significant commitments should be disclosed with an indication of the time involved. Additional external appointments should not be undertaken without prior approval of the board, with the reasons for permitting significant appointments explained in the annual report. Full-time executive directors should not take

⁴⁹ Refer to commentary for Recommendation 2.3 of The ASX Corporate Governance Principles and Recommendations (4th edition).

⁵⁰ Recommendation 2.1 of the ASX Corporate Governance Principles and Recommendations (4th edition).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

on more than one non-executive directorship in a FTSE 100 company or other significant appointment.' Whilst this is not mandatory (the UK have a similar comply or explain approach to Australia), most listed companies do tend to follow what is in the Code in the same way as Australian listed companies apply the ASX Governance Principles and Recommendations.

- Also in the UK, Institutional Shareholder Services (ISS), a major proxy adviser, has a five-mandate limit where a non-executive directorship counts as one mandate, a non-executive chair counts as two, and a position as executive director is counted as three. ISS may vote against directors who appear to hold excessive mandates.⁵¹

This is notable because historically Australian governance has tended to align with changes made in the UK. Indications from APRA that they are concerned about the fact that there is 'little consideration of the capacity of directors to balance multiple roles and professional obligations'⁵² and their proposals to address this are likely to see similar measures brought into APRA regulated entities.

Ultimately, regardless of what is mandated or recommended by regulators, it is sensible to ensure that directors are able to fulfill their duties. In doing so it will be necessary to consider individuals' personal circumstances and approach to work. Thus it is likely that the best measure is how directors are performing, including availability to meet responsibilities as they arise and attendance at meetings. In light of concerns regarding overboarding, boards will be well served to demonstrate that this is a consideration as part of the board performance assessment process.

The commentary for Recommendation 1.6 of the ASX Corporate Governance Principles and Recommendations specifies that 'a suitable non-executive director (such as the deputy chair or the senior independent director, if the entity has one) should be responsible for the performance evaluation of the chair, after having canvassed the views of the other directors'.

The evaluation process

Some of the issues to consider when designing an evaluation include:

- the type of assessment and evaluation process to be used (e.g. qualitative, quantitative or a combination of both)
- the scope of assessment and evaluation
- who should perform the assessment and evaluation process (in-house, chair, external independent facilitator)
- the timing and frequency of the assessment and evaluation.

A gap analysis between how the board or committee actually works and good board practice is a useful starting point for any evaluation. Conducting regular board and committee evaluations also sends a signal to the marketplace that the company is serious about governance and enhancing its performance. Shareholders and proxy voters are beginning to take more notice of whether companies engage in this practice with particular focus applied as to whether an external independent evaluation has been conducted at least every three years.

The commentary for Recommendation 1.6 of the ASX Corporate Governance Principles and Recommendations states that 'the board should consider periodically using external facilitators to conduct its performance reviews'. Consequently, it is now increasingly common for companies to engage an external consultant to facilitate a board review at least every two years, with an internal review usually facilitated by the chair every other year.

⁵¹ <https://www.issgovernance.com/file/policy/active/emea/UK-and-Ireland-Voting-Guidelines.pdf>

⁵² APRA, March 20205, Governance Review Discussion Paper, <https://www.apra.gov.au/sites/default/files/2025-03/Governance%20Review%20-%20Discussion%20Paper.pdf>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

As well as offering independence, an external expert facilitator can help to shine a light on previously unthought-of aspects of the evaluation process that will glean further opportunities for board development and succession planning.

The board or nomination committee can address gaps identified during the evaluation process through professional development and/or succession planning (both of which are covered separately in this chapter).

DIRECTOR REMUNERATION

Non-executive director remuneration – process

Directors are not entitled to payment for services unless this is provided for in the constitution of the organisation or approved in a resolution of shareholders. The Corporations Act provides that 'the directors of a company are to be paid the remuneration that the company determines by resolution'.⁵³ The company 'may' also pay the directors' travelling and other expenses that they properly incur:

- in attending directors' meetings or any meetings of committees of directors
- in attending any general meetings of the company
- in connection with the company's business.⁵⁴

The ASX Corporate Governance Principles and Recommendations also recommends that a board of a listed entity should have a separate remuneration committee as an efficient and effective mechanism to bring the transparency, focus and independent judgement needed to remuneration decisions. The commentary to Recommendation 8.1 also sets out which matters the remuneration committee should consider when making recommendations to the board.⁵⁵

⁵³ Corporations Act 2001, Replaceable Rule Section 202A(1).

⁵⁴ Corporations Act 2001, Replaceable Rule Section 202A(2).

⁵⁵ Recommendation 8.1 of the ASX Corporate Governance Principles and Recommendations (4th edition). Refer to chapter 3.4 for further information on committees.

Companies should clearly distinguish and separately disclose the policies and practices regarding the structure of non-executive directors' remuneration from that of executive directors and senior executives.⁵⁶ The ASX Corporate Governance Principles and Recommendations provide some useful guidance on formulating remuneration policies and practices for both executives and non-executives, in the commentary to Recommendation 8.2. It is critical that the board establishes a process by which directors can determine both their structure and remuneration levels in an objective manner.

For listed companies, the company must obtain shareholder approval for any increase to the maximum aggregate of non-executive director fees, from which fees to non-executive directors for their participation on the board and board committees should be paid (inclusive of superannuation).⁵⁷ The board then determines how this is distributed to individual directors. Many companies obtain by resolution an upper limit to the total amount to be paid on an ongoing basis and then infrequently seek to have this increased. Usually companies do not allocate this total amount. A listed company will need to have sound reasons for seeking an increase to this amount.⁵⁸

Non-executive director remuneration – structure and quantum

Non-executive director compensation should be:

- determined by the board and disclosed completely to shareholders
- aligned with the long-term interests of shareholders
- at a level to adequately compensate directors for their time and effort.

Non-executive directors should normally be remunerated by way of fees, in the form of cash, non-cash benefits, superannuation contributions or salary-sacrifice shares. The AICD supports the view that individual directors should have the freedom to nominate the proportion of their total remuneration that falls into each category.⁵⁹

⁵⁶ Recommendation 8.2 of the ASX Corporate Governance Principles and Recommendations (4th edition).

⁵⁷ ASX Listing Rule 10.17.

⁵⁸ AICD, 2017, Directors' fees, <https://aicd.companydirectors.com.au/resources/Director-tools/practical-tools-for-Directors/board-composition/Directors-fees>

⁵⁹ GIA, Good Governance Guide: Director remuneration – non-executive share ownership, 2012.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

As a general rule, compared with executives, non-executive directors should not receive options or bonus payments which are dependent on the satisfaction of performance conditions, as this can bias their judgement in favour of short-term performance. Non-executive directors should not be provided with retirement benefits (other than superannuation), as entitlements to benefits that accrue over time may discourage directors from retiring or resigning from the board at the most appropriate time.

In setting fee levels, a balance needs to be struck between attracting and retaining highly skilled directors, and paying an appropriate level of fees that properly reflect the responsibilities of the directors (including risks associated with the role and their membership on particular committees), the size and complexity of the company and its operations, the industry sector, the time commitment required of the director, the director's qualifications and experience and any other duties to be carried out within the role (e.g. chair of certain board committees). Larger organisations will often develop a fee system that compensates directors according to the number of subcommittees in which they participate, and whether they participate as the chair or member. This should involve reviewing the director's remuneration annually, and can include a peer group benchmarking review, if warranted.

Some boards also pay a travel allowance where board meetings are held internationally and directors are required to commit to significant travel time to attend meetings.

Many argue that directors should build a material share ownership in the company to directly link directors' interests to those of the shareholders. There is an increasing trend towards companies adopting policies requiring or encouraging non-executive directors to acquire a minimum shareholding in the company. If it is a listed company, the ASX should be notified of those shareholdings within the required timeframe,⁶⁰ noting blackout periods that should be detailed in the listed entity's trading policy.

The GIA provides some useful guidance and basic principles that should be considered in establishing a non-executive director share ownership policy.⁶¹

In some circumstances, such as takeovers and mergers, directors may be required to spend considerably more time reviewing proposals or responding to the situation. In these circumstances, it has become more common for directors to receive additional remuneration to take account of the extra time.

Volunteer board members, including directors of government entities, are often entitled to claim 'reasonable' expenses. The specific details will be outlined in the letter of appointment, supported by the relevant board charter or Enabling Act (whichever applies).

Not-for-profit director remuneration

Not-for-profit organisations may or may not pay directors. Some not-for-profits take the view that directors should see their contribution as service to the community and hence receive no remuneration outside of reasonably occurred expenses. Others, usually larger not-for-profits, take the view that they expect a considerable workload from directors and are seeking directors with high levels of skills. Not-for-profit Director remuneration continues to rise, with the AICD reporting that 24 per cent of directors in their 2025 not-for-profit study were noted to be receiving payment (up from 21 per cent in 2024 and 13 per cent in 2015).⁶² When this is taken across the whole population, the AICD report that nearly half of all NED and chair positions across sectors are unpaid with noted prevalence in the not-for-profit sector.⁶³

61 GIA, Good Governance Guide: Director remuneration – non-executive share ownership, 2012.

62 AICD, 2025, Not-for-Profit Governance and Performance Study 2024-25, March 2025, <https://www.aicd.com.au/board-of-directors/career/salary/aicd-director-remuneration-report-2025.html>

63 AICD, 2025, AICD Director Remuneration Report 2025, May 2025, <https://www.aicd.com.au/board-of-directors/career/salary/aicd-director-remuneration-report-2025.html>

60 Corporations Act 2001, Section 205G.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

When a not-for-profit company is a registered charity, the provisions of the Corporations Act, the Australian Charities and Not-for-profits Commission Act 2012, and the Australian Charities and Not-for-profits Commission (ACNC) Governance Standards must be considered. While not specifically mentioning payment to directors, the ACNC Governance Standard 2 is relevant:

'Charities that have members must take reasonable steps to be accountable to their members and provide them with adequate opportunity to raise concerns about how the charity is governed.'

Under this Governance Standard it can be expected that the charity will seek members' approval of the total amount of the proposed directors' remuneration and provide details, usually as part of the annual report, as to what payments were made to directors. In short, although not legally required, it is recommended that not-for-profits which pay directors adopt many of the practices concerning approval and reporting as apply to listed companies.⁶⁴

EXECUTIVE DIRECTOR REMUNERATION

It is increasingly acknowledged that executive director remuneration should be structured to achieve two main purposes, to:

- align the interests of shareholders and directors; and
- reward executives for their contribution towards the achievement of company objectives.

Remuneration for executive directors (and other executives) should include an appropriate balance of fixed remuneration and short- and long-term performance-based incentives. Commentary to Recommendation 8.2 of the ASX Corporate Governance Principles and Recommendations sets out those guidelines for executive remuneration.⁶⁵

⁶⁴ Australian Charities and Not-for-Profits Commission (ACNC), Meet governance standards, <https://www.acnc.gov.au/tools/topic-guides/governance-standards>

⁶⁵ Box 8.2 / Suggested guidelines for: Executive remuneration; Non-executive director remuneration, ASX Corporate Governance Council's, Corporate Governance Principles and Recommendations, 4th Edition.

REMUNERATION REPORT – 'TWO-STRIKES' RULE

Listed companies must account annually for directors' fees as well as the remuneration paid to senior management under Section 300A of the Corporations Act.

The Act was amended from 1 July 2011 to provide for the 'two-strikes' rule in relation to the remuneration report. This rule was designed to hold the board to account for executive remuneration. At the AGM, the shareholders must vote approval or otherwise of the remuneration report. The first strike is when a company's remuneration report receives a 'no' vote of 25% or more. Where this occurs, the company's subsequent remuneration report must explain whether shareholders' concerns have been taken into account, and either how they have been taken into account or why they have not been taken into account.

The 'second strike' occurs where the company's subsequent remuneration report receives a 'no' vote of 25 percent or more. Where this occurs, shareholders will vote at the same annual general meeting to determine whether the directors will need to stand for re-election within 90 days. If this resolution passes with 50 percent or more of eligible votes cast, then the 'spill meeting' will take place within 90 days. At the spill meeting, those individuals who were directors when the report was considered at the most recent annual general meeting will be required to stand for re-election (other than the managing director, who is permitted to continue to run the company).⁶⁶ There has been an uptick in the number of companies who received a strike on their Remuneration Report, with a record-breaking 11% of the ASX 100 companies receiving a 'no' vote in FY23 and 25% of the ASX 200 receiving strikes in FY24.

⁶⁶ AICD, Director Remuneration, <https://aicd.companydirectors.com.au/resources/all-sectors/Director-remuneration>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The most common reasons observed for remuneration report strikes are as follows:

- Executive bonus outcomes not aligned with business performance/ shareholder outcomes.
- Overall quantum of remuneration is too high or misaligned to the company size and performance.
- The executive remuneration structure is viewed as inappropriate (e.g. incentives are not performance tested, ad hoc awards are paid, boards apply upward discretion in a manner deemed too generous or which is poorly explained).
- Failure to exercise board discretion appropriately in the context of regulatory, reputation or other matters (e.g. fatalities).
- Overall dissatisfaction with performance of the company, board or strategic direction of the business (e.g. shareholders using the remuneration report resolution as an opportunity to demonstrate discontent with company matters more broadly – for example, too many executive changes and instability in the executive team – rather than just on executive remuneration).

RE-ELECTION AND ROTATION OF DIRECTORS

For non-listed companies, the requirement and terms of the re-election of directors is dependent on the company's constitution.

For listed companies, ASX Listing Rules 14.4 and 14.5 require all directors, other than the managing director, to stand for re-election at the company's AGM at least once every three years. ASX Listing Rule 14.3 requires that a company must accept nomination for the election of directors up to 35 business days prior to the AGM, unless the company's constitution provides otherwise.

Recommendation 1.2 of the ASX Corporate Governance Principles and Recommendations recommends that for directors standing for re-election, the board should provide the security holders with details of the term of office currently served by the director and, if the candidate standing for re-election is to be an independent director, a statement to that effect and a statement by the board as to whether it supports the re-election of the candidate and its reasons why. The board should also consider the evaluation of the candidate's independence when providing details. Further details can be found in the 'Board Evaluation' section of this chapter.

BOARD SUCCESSION PLANNING

Board succession planning challenges boards to anticipate and plan for their future needs. It should be a continuous process that is regularly considered by the board so that changes in the board composition can be anticipated and planned for in advance.

Its role in the company's strategic success has increased in significance due to the increased pressure for non-executive directors to limit the number and tenure of directorships as described earlier in this chapter.

Recommendation 2.1 of the ASX Corporate Governance Principles and Recommendations sees 'board succession planning generally' as one of the roles of the nomination committee.

Board succession planning is built on:

- an assessment of the challenges and opportunities facing the company, now and in the future (and therefore strongly aligned to the strategy development process)
- an analysis of the core skills, competencies and behaviours that are required, both immediately and in the future, for both the board and its committees
- an evaluation of the skills, competencies and behaviours of existing directors, including their strengths and weaknesses, skills and experience gaps, current age range and gender composition, and length of tenure
- assessments of existing directors' performance
- assessments of non-executive directors' independence.

Recommendation 1.5 of the ASX Corporate Governance Principles and Recommendations states that gender diversity should also be a relevant consideration in succession planning.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Succession planning for chairperson

In developing a succession plan, the chair's role needs to be considered by the board or nomination committee. In instances where the current chair's retirement date is known, plans can be set in place to identify a new chair, either internally or externally.

Companies should also have a contingency plan for the chair's role, in the case of some unexpected event. Previous cases of simultaneous vacancies in the roles of both the chair and managing director are a reminder to all boards of the consequences of such unplanned disruptions to a board's succession.

DIRECTOR TENURE

KPMG Enterprise's report, *Secrets to success of the ASX 300+: Six priorities of opportunity and challenge* found that in 2016, companies with a chairperson of 10 years or more tenure delivered significantly better financial performance in terms of revenue growth compared to the rest of the group surveyed. This helps to understand the resistance to challenge these long-held appointments and potentially disrupt the company's successful financial strategy. However, as identified in the report, a key challenge facing these companies is the risk of becoming stale through a lack of diversity of thought and opinion.

In APRA's 2025 Governance Review Report, APRA describes that one of the proposals that they are seeking to address areas of persistent concern is to impose a lifetime default tenure limit of 10 years for non-executive directors at a regulated entity. This is based on the report highlighting that 12% of regulated entities had tenure of directors on boards in excess of 10 years with 8% exceeding 12 years.⁶⁷ This is not out of line with what is expected globally, for example,

- the Hong Kong Stock Exchange (HKEX) introduced a 9-year tenure limit for Independent Non-Executive Directors (INEDs) as part of its Corporate Governance Code enhancements, which were finalised in December 2024 and took effect on 1 July 2025;

- the UK Corporate Governance Code similarly states that after nine years of service, an INED is no longer considered independent. The chair of the board is also subject to the nine-year independence threshold and this includes all time served on the board, not just time as chair.⁶⁸ This is however under a comply or explain regime whereas the HKEX requirements are mandatory.

As stated in the Succession Planning section of this chapter, the commentary for Recommendation 2.1 of ASX Corporate Governance Principles and Recommendations states that 'board renewal is critical to performance'. There is a danger that longstanding directors become entrenched and lose their ability to consider issues from an impartial and objective standpoint. Tenure has been cited as one of the key criteria for evaluating the independence of NEDs in the ASX Corporate Governance Principles and Recommendations;⁶⁹ for this reason, many listed companies adopt a director tenure policy providing for a maximum term of office (e.g. nine years being three terms of three years each), with any extension being subject to annual approval. A company's constitution can also provide for situations in which a director's office is to be vacated at any given point in time (e.g. unsoundness of mind).

A director may resign by giving notice in writing to the company, unless the company's constitution provides otherwise.⁷⁰

The company must notify ASIC of the resignation within 28 days.⁷¹

Removing a director who is unwilling to leave is a difficult situation. By law, the directors of a public company cannot pass a resolution requiring a director to vacate office;⁷² only by resolution of a general meeting can the company remove a director.⁷³ The law prescribes a process for the removal in which the director has a right to put their case to the members.⁷⁴

68 https://media.frc.org.uk/documents/UK_Corporate_Governance_Code_2024_a2hmQmY.pdf

69 Refer to Recommendation 1.6 of ASX Corporate Governance Principles and Recommendations (4th edition).

70 Corporations Act 2001, Replaceable Rule Section 203A.

71 Corporations Act 2001, Section 205B(5).

72 Corporations Act 2001, Section 203E.

73 Corporations Act 2001, Section 203D.

74 Corporations Act 2001, Section 203D(4).

67 APRA, March 2025, Governance Review Discussion Paper, <https://www.apra.gov.au/sites/default/files/2025-03/Governance%20Review%20-%20Discussion%20Paper.pdf>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ACCESS TO COMPANY RECORDS

The Corporations Act provides that directors (both current and former) have a legally enforceable right of access, at all reasonable times, to the company's books for the purposes of a legal proceeding:

- to which the director is a party;
- which a former director proposes to bring in good faith; and
- which a director has reason to believe will be brought against them.⁷⁵

This right extends for a period of seven years after the person ceases to be a director of the company, and also includes the right to inspect the company's financial records.

It is generally established practice for:

- directors not to retain individual copies of board papers; and
- a deed of access between the company and each director to be executed, which sets out the rights of the director to access board papers and/or company information and how such information may be used.⁷⁶

The board could consider adopting an information policy which provides that the company secretary holds a complete set of board and committee papers. Under this policy, directors should be entitled, on request, to access board papers for the period during which they were a director, even if they have ceased to be a director. Increasingly, such papers are being held electronically, with approval granted to directors, enabling easy access and avoiding the need for the retention of papers by individual directors.

⁷⁵ Corporations Act 2001, Section 198F(1).

⁷⁶ Corporations Act 2001, Section 198F(2).

Useful resources

- *Corporations Act 2001*
- ICSA Guidance Note, 2021, Due Diligence for Prospective Directors.
- AICD, Appointing a New Director: Role of the Board, <https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/stakeholder/appointing-a-new-director-director-tool.pdf>

For further information please contact:



Andrew Holland
Partner, Performance
and Reward
KPMG Australia
aholland1@kpmg.com.au



Caron Sugars
Lead Partner,
Board Advisory Services
KPMG Australia
ccobargsugar@kpmg.com.au

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

10. Company Leadership

Most boards would agree that one of their most important governance roles is hiring and, when required, replacing the CEO. After all, the CEO is responsible for the day-to-day operations of the organisation and is instrumental in both the development and execution of corporate strategy.

In this chapter

- CEO and executive management
- Executive remuneration
- Role of the CEO
- Executive service agreements

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Does the board have confidence in the skills and capabilities of the CEO and the senior management team? What process or approach is in place to help to objectively validate this view?
2. How does the CEO encourage and support the talent pipeline through attraction, development and retention of high potential employees?
3. What is the 'tone at the top', as understood and experienced by layers below?
4. Does the board have a CEO and senior management succession plan that is regularly (e.g. semi-annually) considered and reviewed for relevance, given the operating environment of the organisation at the time of review (such that talent is considered in the context of the current and prospective operating environment)?
5. Does the board have in place a robust and fit-for-purpose succession readiness program that is ready to support a CEO replacement process at any time and is supported by internal executive talent development?
6. Prior to the appointment of a new CEO, does the board (through the chairperson or nomination committee) conduct a rigorous succession evaluation process?
7. Is the CEO's view regarding senior management team members and other talented people with strong leadership qualities considered?
8. Are concerns about the CEO's performance discussed with the CEO and appropriately documented?
9. Does the board have a transparent process for determining management remuneration (both in respect of base salary and incentive arrangements)?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The CEO selection process was conducted largely in-house within a pool of board members' friends and business associates.
- Support and confidence in the CEO is divided amongst board members.
- The CEO does not have KPIs or they are often not being met.
- Remuneration setting is mostly discussed privately.
- CEO performance appraisal is conducted infrequently and informally.
- No contingency plan or succession plan exists for the current leadership structure; or the plans that do exist lack substance and meaningful engagement (i.e. box checking).
- The CEO seems focused mostly on achieving their own remuneration and incentive targets.
- There is no senior executive development plan in place.
- There is no regular review or external assessment of senior executive talent.
- The board has restricted or no access to senior management.
- The board is often drawn into operational matters due to lack of confidence in and/or capability of the executive.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

CEO AND EXECUTIVE MANAGEMENT

The CEO should be involved in nearly all board discussions and have input into decisions, where appropriate. They should also have meaningful delegated authority to enable the execution of the enterprise's strategy. The CEO is pivotal to establishing and reinforcing to all stakeholders the 'tone' of what is expected of the enterprise; they play a key role in representing the organisation to external parties.

It is usual practice for a CEO to establish an executive management team (or similar) which will:

- provide support to the CEO
- exchange information and ideas
- constructively develop and implement strategies and management frameworks
- provide input on the organisation's direction
- influence the organisation at all levels.

Building a strong executive management team is essential for organisational success. Factors associated with strong organisational leadership include:

- board and management roles and responsibilities clearly delineated and articulated in writing
- board protocols covering directors' access to executive managers outside of board meetings
- a CEO that provides appropriate direction, mentoring, support and guidance to executive management team members
- executive management team members who are empowered to share leadership responsibilities
- executive management team members who are rewarded for organisational, business unit and individual performance, based on behavioural standards displayed and value creation outcomes
- management succession and development plans that cover all key positions, based on competencies, behaviours and experience to achieve the strategic vision
- full disclosure of conflicts of interest.

'Leaders establish the vision for the future and set the strategy for getting there; they cause change. They motivate and inspire others to go in the right direction and they, along with everyone else, sacrifice to get there.'

Dr John Kotter, Konosuke Matsushita Professor of Leadership, Emeritus, Harvard Business School

ROLE OF THE CEO

It goes without saying that, as a company's most senior officer, the CEO is critical to the performance of the enterprise. The scope of activities and responsibilities assigned to the CEO are broad and far-reaching. Through their attitudes and behaviours, CEOs are instrumental in reinforcing the 'tone' of their organisations.

An effective CEO:

- leads with clear purpose and actions this purpose through providing clarity to the organisation
- actively develops direct reports and sponsors organisation-wide people development
- is consultative, as well as courageous, in making the decisions needed
- always acts with integrity
- drives strategic vision and innovation
- is resilient in the face of setbacks
- successfully adapts to the company's ever-changing circumstances
- demonstrates high-level business acumen
- meets immediate performance targets without neglecting longer-term growth opportunities.

While the titles CEO and managing director (MD) are often used interchangeably, the key difference is that a CEO does not necessarily have a seat on the company's board, whilst the MD is, by definition, also a director of the company.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Delegated authority

There should also be a formal statement delineating the boundaries between board and management responsibilities, including the board's retained authorities and those delegated to management. This is usually set out in the board charter.

A high-performing board will invest time and effort in constructing an active partnership with the CEO and senior management. It will not be a relationship based mainly on supervision but one in which the board engages with the CEO and senior management to achieve outstanding results.

In putting its relationship with the CEO on a sound footing, a board needs to formulate a CEO's job description and define the criteria for assessing the CEO's performance, which will typically then underly any performance-tested remuneration.

Outside directorships

Traditionally, the CEOs of many of Australia's leading companies were invited onto the boards of other public companies. The only real restriction on this practice was the avoidance of overt conflicts of interest. This practice was not considered exceptional, and was seen as a good training ground for public company directors. In recent times, the size of current CEO remuneration packages and the scope of their responsibilities, has often made outside directorships untenable.

It is not uncommon for CEOs who are coming to the end of their management tenure to seek out unrelated non-executive directorship. Proxy advisors appear to be comfortable with this approach for transitioning CEOs although some do suggest limits (such as no more than one or two boards) to ensure the board role is given the necessary attention appreciating the workload that a CEO will have already.

Former CEOs can make excellent non-executive directors in other companies. However, many who have made the move report that there is a significant transition from being a CEO wielding considerable power and influence to the collegiate and consensus-based role of the non-executive director. This is where having a clear understanding of the role of a director (versus being part of the executive team) is crucial for both the board and management to effectively do their jobs.

It is no longer common practice for retiring CEOs to remain on their boards in a non-executive capacity, or for retiring CEOs to assume the chair's role as it then raises issues of independence. According to the ASX Principles, a director who was previously employed in an executive capacity by the company (or another group member) will generally not be considered independent unless a period of at least three years has lapsed between the director ceasing such employment and serving on the board.¹

CEO succession planning

The purpose of succession planning is to ensure the board always has available a number of successor candidates in the event that the incumbent CEO departs suddenly and unexpectedly. Ideally, succession planning should start from day one of a new CEO's appointment.

Each company's needs are unique and change over time, as does the available pool of talent from which a new CEO may be drawn. The board should ask the CEO to provide an assessment of the key internal contenders and what is being done to develop their strengths and overcome any limitations in order to prepare them for being succession ready.

Some companies approach succession planning by considering different contingencies, ranging from crisis management (e.g. If something untoward were to happen to the CEO, could the company continue to operate successfully?) to long-term issues such as attraction, development and retention of individuals to be future leaders.

¹ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2014, Recommendation 2.3, Box 2.3 which sets out the 'Factors relevant to assessing the independence of a director'. In each case, the board must assess the materiality of each such factor and determine whether the director has the capacity to bring an independent judgement to bear on issues before the board and to act in the best interests of the entity as a whole.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

At the heart of CEO succession planning is the notion that the board and the CEO work in cooperation to attract, develop and retain high performers who can be tried and tested prior to possibly being offered the CEO role in the future.

Selecting a CEO

The selection of a CEO is the most important task a board can undertake. It is also probably the most difficult. Boards should drive the succession process, although normally in collaboration with the incumbent CEO. Boards sometimes select a CEO 'heir apparent' well in advance of the incumbent CEO's planned departure.

For organisations with good succession planning, the selection of a CEO may appear almost automatic with a suitable successor long identified. However, as executives become more mobile and the typical CEO's job tenure continues to shrink, conventional succession planning may not identify an unequivocally acceptable internal candidate. Many boards will feel they have an obligation to look beyond a company's own executive ranks if they are to find the best available CEO.

The board must ensure that robust processes are adhered to in the lead-up to the appointment. Experience suggests that the probability of a successful outcome is enhanced if boards follow a structured appointment process.

Confidentiality is critical throughout the appointment process. Any breach will deter potential candidates and reflect poorly on directors and the company as a whole.

CEO tenure

CEOs are increasingly under the spotlight with boards being prepared to replace them if they consider that their CEO is not performing, or believe that future performance may not be up to the level expected.

Investment in the CEO and management team is crucial for the creation of sustained shareholder wealth. In their article titled *More and Better Options: Strengthening Long-Term CEO Succession Planning*, the Harvard Law School Forum on Corporate Governance noted three barriers to creating successful CEO succession pipelines, namely:

- being underprepared for emergency CEO situations;
- not looking far enough into the future; and
- hesitating to put the C-suite succession pipeline under the microscope²

For this reason, directors need to commit considerable time and effort to selecting a new CEO. The best time to start succession planning is the day after a CEO begins their tenure. This should be supplemented by appropriate mentoring, development, encouragement and support of the incumbent CEO; a role often fulfilled by the chair of the board.

CEO appraisal

The CEO performance appraisal is an important board responsibility and should take place on an annual basis. This appraisal provides:

- important feedback to the CEO about their performance
- increased understanding of the CEO's concerns and views on the achievement of corporate objectives
- a forum to build a healthy relationship between the board, especially the chair, and the CEO
- a framework for the CEO to further develop capabilities
- a forum to reinforce accountability, transparency and the responsibilities of the CEO
- an opportunity to identify and address early warning signs of possible difficulties
- an opportunity to discuss any future plans the CEO may have (e.g. retirement).

² Posted by Rusty O'Kelley, Margot McShane, and Justus O'Brien, Russell Reynolds Associates, on Sunday, July 26, 2020. <https://corpgov.law.harvard.edu/2020/07/26/ceo-succession-plans-in-a-crisis-era/>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

A robust appraisal process should be established that reflects the company's unique circumstances. This work is generally the responsibility of the remuneration committee, which will make recommendations to the entire board.

A more accurate picture of CEO performance can be gained by incorporating the views of several groups. For example, directors, senior executives, institutional shareholders, customers, suppliers and other key stakeholders will all have a view on the CEO's performance. This must be handled sensitively and all comments treated confidentially to uphold the integrity of the appraisal process.

Both quantitative and qualitative indicators may be included to assess the CEO's leadership behaviour and performance goals, which are fundamental to sustained organisational performance. Using financial and company performance measures alone are inherently problematic. There is an array of factors outside the direct control of the CEO that can affect company performance. A CEO may be performing strongly when the company is not and vice versa. Also, shareholder value can be measured from a number of perspectives, with startlingly different end results. In any event, CEO performance should be measured not only against short-term company financial performance, but also on the CEO's own performance, especially against agreed key performance indicators and corporate strategic objectives.

When CEO performance concerns arise, these should be discussed and addressed promptly. If it is clear that the CEO is not delivering and needs to be replaced, then the board should act without delay. Whilst the cost of replacing a CEO is considerable, the cost of not acting can be devastating.

EXECUTIVE REMUNERATION

Executive remuneration is a topic that usually elicits much discussion and controversy. ASX Principle 8 provides that a company should remunerate fairly and responsibly. In determining a remuneration policy, the board needs to:

- ensure that remuneration is set at levels that appropriately reward, motivate and incentivise management to execute company strategy
- demonstrate a clear relationship between senior executives' performance and remuneration
- ensure that the remuneration policy is understood by investors.

Executive remuneration should include an appropriate balance of fixed and variable remuneration. Commentary to Recommendation 8.2 of the ASX Principles sets out the guidelines for executive remuneration, including:

- fixed remuneration should be fair in light of legal, labour and market conditions and relative to the scale of business operations
- variable remuneration should be clearly linked to specific performance targets, appropriate to the company's objectives, goals and risk appetite
- equity-based payments may be an effective form of remuneration to align executives' incentives with long-term company performance
- termination payments must be agreed in advance and no payment should be made in the case of misconduct.

Section 300A of the Corporations Act requires listed companies to make specific and comprehensive annual disclosures regarding the company's remuneration framework and the remuneration arrangements for the key management personnel (KMP). At each annual general meeting, shareholders of listed companies have the opportunity to vote on the company's remuneration report. The two strikes rule is discussed in further detail in [Chapter 9](#).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Typically approaches see executive remuneration delivered in the following components:

- Fixed remuneration (e.g. salary, superannuation, fringe benefits).
- Variable remuneration, consisting of:
 - Short term incentive (e.g. at-risk remuneration with vesting assessed against financial and non-financial measures (typically via a balanced scorecard) over the financial year). Depending on the role eligible to participate in the STI, performance may be assessed against specific or individual measures. The STI may be settled in cash or equity or both.
 - Long term incentive (e.g. at-risk remuneration with vesting against company-wide measures – typically linked to share price return, long term financial metrics of success, strategic milestones and ESG). The LTI is designed to align executives with shareholders and the long term performance of the company and is typically assessed over a 3 – 5 year period.

The challenge for boards is to identify and implement a remuneration framework which best supports the organisation's ability to achieve its unique business strategy.

Benchmarking remuneration and incentives against other similar organisations is a common method used to gauge the appropriateness of base salary and incentive arrangements and inform remuneration decisions.

Shareholders demand that the process for setting remuneration be transparent and as detailed in [Chapter 11 Board Committees](#), certain procedures are required to be followed when engaging a remuneration consultant to provide a recommendation in relation to the quantum or elements of KMP remuneration to ensure that the remuneration consultant is free of undue influence by the KMP to whom the remuneration recommendation relates.³

Other measures implemented by the Australian Government in response to perceived corporate excess included the significant tightening of restrictions relating to termination payouts or 'golden handshakes'. Broadly termination payments for regulated executives cannot exceed one times an executive's base salary without shareholder approval being obtained.⁴

EXECUTIVE SERVICE AGREEMENTS

Listing Rule 3.16.4 requires an entity to disclose the material terms of any employment or service contract (or any variation to it) with the CEO (or equivalent) and any of its directors.

With more rigorous disclosure requirements, the board's approach to negotiating the terms of CEO and senior executive service contracts is more open to challenge by the media and shareholders.

The board has the difficult task of striking a balance between the need to attract and retain senior executives with protecting company interests. Most importantly, the process by which executive service agreements are set up must be transparent and beyond reproach.

The remuneration committee is usually vested with the responsibility of providing recommendations to the board in relation to the key terms of executive service agreements and remuneration arrangements on appointment. It is important that there is sufficient expertise within the ranks of the remuneration committee to effectively advise the board on these matters, and to seek external advice as required. The board is ultimately responsible for ratifying the appointment of the CEO, and thus it should retain sign-off authority.

³ Corporations Act 2001, Section 300A(1)(h).

⁴ Corporations Act 2001, Sections 200B and 200F.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

It is important that the process adopted ensures the executives for whom contracts are being negotiated remain at arm's length (i.e. instructions on the preparation of the contract should be given directly to solicitors or consultants by the remuneration committee). This does not preclude the CEO and other senior executives from making submissions to the remuneration committee about their own contracts or making recommendations on the remuneration of their direct reports.

The preparation of an executive service agreement is complex. Professional advisers should be engaged who can ensure that the contract reflects what has been agreed and that the contract accords with the law and appropriately protects the company's interests. Any drafting of contracts needs to consider the regulatory framework and the company's governing documents, including:

- Corporations Act (particularly Part 2D.2)
- ASX Listing Rules
- industrial relations, employment and WH&S legislation
- company constitution
- company remuneration policies.

For general guidance of what should be included in an executive service agreement, refer to the ASX Principles commentary to Recommendation 1.3.

Useful resources

- KPMG, 2023, Insights into Remuneration Reporting [Remuneration Reporting Guide – KPMG Australia](#)
- KPMG, 2023, ESG in Executive Remuneration [ESG in executive remuneration – KPMG Australia](#)

For further information please contact:



Andrew Holland
**Partner, Performance
 and Reward**
KPMG Australia
aholland1@kpmg.com.au



Caron Sugars
**Lead Partner,
 Board Advisory Services**
KPMG Australia
ccobargsugar@kpmg.com.au

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

11. Board Committees

Board committees can enhance the oversight provided for companies. As increasingly more is being required from boards, greater use is being made by committees to help all directors better perform their duties and discharge their responsibilities in an effective and efficient way.

In this chapter

- Types of committees
- Benefits of committees
- Committee charters
- Committee annual agenda
- Committee induction framework
- Committee meeting agenda and minutes
- Committee size and composition
- Committee/board interaction and reporting
- Committee evaluation
- Typical committees of the board
- Audit committee
- Risk committee
- Remuneration committee
- Nomination committee
- Sustainability committee
- Other common committees
- Special purpose committees

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Do the committees in place help the board focus on the key risks and issues facing the organisation?
2. Are board committee charters approved by the board and reviewed annually?
3. Are board committees comprised of a majority of independent directors?
4. Are the chair of the board and the chair of the audit committee different people?
5. Are the chair of the board and the chair of the remuneration committee different people?
6. Does each board committee have the expertise and experience to properly advise the full board?
7. Are there an appropriate number of directors with accounting or financial expertise on the audit committee?
8. Does the audit committee meet without management present in order to question the external and internal auditors?
9. Does the board critically scrutinise and question the information provided, and recommendations made, by a board committee, even when endorsed by 'experts'?
10. Are non-financial risks given as much attention as financial risks in risk committee meetings?
11. Are separate committees required in order to address ESG and/or other emerging requirements?
12. Is the board informed of any issue upon which committee members are not in full agreement?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- Board committees lack terms of reference or charters.
- Certain committees are not resourced with appropriately skilled people.
- The audit committee meets only when required by internal or external auditors.
- Minutes are not taken at committee meetings or the minutes are not distributed regularly to members.
- The audit, nomination or remuneration committee involve mostly executive directors due to the unavailability of independent directors.
- The audit committee has little to do with assessing internal control systems and coordinating with the internal audit function.
- Only financial risks are discussed in the risk committee.
- Similar sized companies or competitors have established additional committees that the company is yet to establish.
- There is irregular reporting to the board from the chairpersons of the committees.
- There is insufficient detail provided by the committee chairman for the issues to be appropriately considered.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

THE ROLE OF COMMITTEES

Committees play a critical role in managing the work of the board, providing the opportunity for directors to focus on specific areas of compliance and performance across a range of areas. Within the context of dynamic risk environment, greater regulatory scrutiny and heightened stakeholder expectations of company performance and disclosures, the agendas of many boards and their committees are becoming very full.

Consequently, committee structures and processes are increasingly being reviewed to ensure that they remain 'fit for purpose', in that they are adaptable to current and emerging issues and are agile in how they work to strike the balance between hindsight, insight, oversight and foresight as and when required.

This is giving rise to boards questioning things such as:

- What are the most appropriate committees for our organisation?
- How do we determine the right committee structure given the range of issues we need to be across?
- What is the right level of information that we should be getting in committee reporting?
- What information is relevant for reporting and escalating through to the board?
- How can we streamline the information – particularly compliance information – to allow us greater time for future-focused and strategic discussion?

Answering these questions requires looking at the core enablers of organisation success, clarifying what is the remit of the board versus what are issues for management and defining what information is needed to gain comfort that compliance obligations and performance expectations are being met.

TYPES OF COMMITTEES

The most common board committees are:

- Audit (and risk management) committee
- Nomination committee
- Remuneration committee.

Depending on circumstances, additional committees, including ad hoc committees, may be established to deal with other pertinent matters, oversee specific projects or focus on key risk areas for the organisation.

Types of additional committees can include sustainability, people, safety, technology, research and development and special purpose (e.g. takeover and merger). However, in general terms, the number and scope of board committees will depend upon the size and complexity of the organisation.

Whilst committees may be named differently or might be combined to meet the needs of the board and the organisation (e.g. an audit and risk committee in one organisation may be a risk and audit committee in another and an audit, risk and governance committee in a third), the important point is that the committee meets the needs of the board and is clear on its mandate. Combined committees should ensure that the agenda is structured to allow for meaningful discussion of all areas within the committee's mandate and may require a rotating order of items to ensure that important matters scheduled at the end of the meeting are not rushed or overlooked.

The most commonly understood committee names are used in this chapter, consistent with the ASX Principles and Recommendations.

Audit committee

Listing Rule 12.7 requires ASX listed companies included in the S&P/ASX 300 index to have an audit committee. Recommendation 4.1 of the ASX Principles also suggests that a listed entity have an audit committee.

Stakeholder expectations of audit committees have increased significantly, both in Australia and internationally.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The commentary to Recommendation 4.1 of the ASX Principles lists those matters for which the audit committee should make recommendations to the board. Most audit committees perform the following functions:

- reviewing financial statements and other financial information distributed externally
- monitoring company financial reporting to ensure compliance with the Corporations Act, ASX Listing Rules and other regulatory requirements
- reviewing the nomination and performance of the external and internal auditors
- making recommendations relating to the appointment and removal of external and internal auditors
- overseeing and considering the effectiveness of internal control systems
- assessing the performance and objectivity of the internal audit function.

It is fundamental that the audit committee has the technical skills and expertise to discharge its responsibilities and the members exercise independent judgement. Above all, audit committee members must act with integrity and honesty.

ASX Principles suggest that the audit committee should include members who are financially literate and consist of at least three members, all of whom are non-executive directors and a majority of whom are independent directors.¹

The external auditor performance evaluation must be based on the committee's view of the external audit process and should include assessments from management and internal audit.

The external auditor should also be given the opportunity to discuss the findings of the committee's evaluation.

¹ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 4.1 and Commentary; KPMG, 2019 Priorities for Boards and Audit Committee, <https://home.kpmg/us/en/home/insights/2019/02/2019-issue1-article2.html>

Where an audit committee is not established, it is crucial the company put in place an alternative means of scrutinising the financial reporting system and the board allocates appropriate time to this function.

Audit committees should continually seek to improve their effectiveness through improving and updating committee agendas. Greater focus should be given to material issues rather than 'checklists' that add little or no value. Audit committees should always be seeking better information flow, through high quality resources and greater internal transparency.

As economic uncertainty, globalisation and geopolitical turbulence continues, audit committee priorities are currently as follows:

- Risk management – with the complexity and interconnectivity of risk, creating a need for multidimensional risk analysis and treatment, rather than the traditional two-dimensional, linear approach most organisations currently apply.
 - When audit and risk committees are separate, it is important to ensure that relevant insights and updates are shared across the committees through regular written or verbal updates from members.
 - Internal audit can maximise its value by focusing on critical risk (operational and financial) and the adequacy of the company's risk management processes generally.
- Tone at the top – culture and short-termism are major challenges and focus on ethics and compliance is important.
- Capability – CFO succession planning and bench strength in the organisation.
- Disclosures – how the external disclosures (including climate-related and sustainability related financial disclosures, as well as non-financial disclosures pertaining to ESG issues such as modern slavery) can better tell the company's story.
- Tax – global tax developments and risks are important to stay appraised of given that tax is an important element of ESG.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

- Technology – risks and opportunities more broadly through technology but also how technology is impacting the finance function's talent, efficiency, and value-add.

Risk committee

Recommendation 7.1 of the ASX Principles recommends that the board should have a committee to oversee the management of risk. If a risk committee is established, its charter needs to be developed with reference to the intersection between its duties and those of other committees, particularly the audit committee. The ultimate responsibility for risk oversight rests with the full board, regardless of whether or not a separate risk committee is established.²

KPMG's model of risk governance considers risk from two angles – risk content and risk process.

- Risk content involves the identification of specific enterprise-level risks that threaten the company's existence, strategy and business model.
- Risk process refers to how the organisation identifies, evaluates, assigns responsibility and reports on risk content.

It is critical that the board has oversight and ownership of the framework that describes how the risk processes are structured and how risk content is identified and managed, including having assurance over the effectiveness of the controls in place to manage risks.

Risk committees generally have the following responsibilities:

- endorsing the risk management policy for approval by the board
- overseeing the establishment and implementation of the risk management framework
- reviewing management's plans for mitigation of the material risks faced by the company
- monitoring emerging risks and changes in the risk profile
- promoting awareness of a risk-based culture.

The commentary to Recommendation 7.1 of the ASX Principles lists those matters on which the risk committee should make recommendations to the board.

Recommendation 7.2 suggests that the board or the risk committee annually review the company's risk framework and disclose at the end of each reporting period whether or not such a review has taken place.

Importantly, there is a need to ensure clarity over the strategic and evolving risks that the board and risk committee need to be actively monitoring and those that are more operational in nature and within the remit of management to manage. KPMG recommends that in reviewing material business risks against risk appetite that the risk committee should also understand what assurance is being received from the three lines (refer [Chapter 15](#)) so as to be informed as to whether determinations pertaining to the rigour of the control environment used to determine risk ratings have been tested.

Outside of companies in the financial services sector, risk committees are most commonly combined with the audit committee.

Under the Australian Prudential Regulation Authority (APRA) framework, the requirements for the composition and charter of a board risk committee are primarily set out in Prudential Standard CPS 510 Governance and supported by CPS 220 Risk Management. The requirements and salient points are as follows:

- The committee is responsible for objective non-executive oversight of:
 - the institution's risk management framework
 - implementation and ongoing operation of risk controls
 - endorsement of the Chief Risk Officer (CRO) appointment or removal.
- The committee must be comprised of non-executive directors, with a majority being independent.
- The chair of the risk committee must be an independent director, and cannot be the chair of the board.

² ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 7.1.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

- The CRO must attend all relevant sections of risk committee meetings and be independent of business lines, finance, and audit.
- While APRA prefers distinct charters for the risk and audit committees, it does not prohibit overlapping membership.

Remuneration committee

The Listing Rules require ASX listed companies in the S&P/ASX 300 Index to have a remuneration committee comprised solely of non-executive directors.³ Recommendation 8.1 of the ASX Principles also recommends that a listed entity have a remuneration committee of at least three members.

A remuneration committee provides support and advice to the board on:

- the company's remuneration framework, recruitment, retention and termination policies and procedures for senior executives, including the process for setting remuneration and assessing performance
- the level and composition of a senior executive's remuneration
- superannuation arrangements
- the remuneration framework for directors.⁴

The commentary to Recommendation 8.1 of the ASX Principles lists those matters for which the remuneration committee should make recommendations to the board.

Companies should limit the use of executive directors serving on the remuneration committee in order to address the potential for, or perception of, conflict of interest. The committee can consult with individual executives on remuneration policies generally, but no individual should be directly involved in deciding their own remuneration.⁵

³ ASX Listing Rule 12.8

⁴ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 8.1 and commentary; Governance Institute of Australia, The Role of the Remuneration Committee, Good Governance Guide.

⁵ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Principle 8.

A key task of the remuneration committee is to monitor levels of remuneration across relevant industries, and the economy as a whole, in order to ensure the company's remuneration policies are effective in attracting, retaining and motivating the people integral to its success.

Remuneration committees are increasingly engaging external consultants to advise on remuneration arrangements, and must take into account the relevant Corporations Act requirements which apply to such engagements.⁶ In summary, these require that:

- The details of the remuneration consultant be disclosed together with related fees and whether the consultant provided any other services to the entity for the financial year. If other services were provided, the nature and amount payable is required to be disclosed such that independence of the consultant is transparent.
- The appointment of remuneration consultants be made directly by the remuneration committee (or the board) to avoid undue influence from key management personnel (conflict of interest).
- The board must include a statement in the annual report to the effect that they are satisfied recommendations have been made by the consultant free from undue influence from the key management personnel to whom the recommendation relates. This should include how they arrived at this determination.

Nomination committee

Recommendation 2.1 of the ASX Principles suggests that the board should establish a nomination committee to oversee a formal, rigorous and transparent process for the appointment and reappointment of directors to the board.⁷ In smaller companies, this function may be performed by the full board or combined with the remuneration committee.

⁶ Corporations Act 2001, Section 300A (1)(h). See Chapter 3.2 (Company Leadership)

⁷ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendation 2.1.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Nomination committees are generally responsible for:

- devising criteria for directorship (including membership of board committees)
- identifying suitable candidates for appointment to the board
- undertaking appropriate succession planning for the board and the CEO as well as providing oversight in relation to succession planning of the executives more broadly
- developing and managing the process for the performance evaluation of the board, committees and directors.

The commentary to Recommendation 2.1 of the ASX Principles lists those matters for which the nomination committee should make recommendations to the board.

Prior to recruiting new directors, the committee would typically undertake a formal process of reviewing the balance and effectiveness of the existing board, identifying the skills and experience needed and considering board candidates who might best provide them.

Ensuring robust board and committee succession plans are in place and that these plans are effective in delivering directors with the required expertise, is another key role of the nomination committee.

Developing a pipeline of future potential board candidates, meeting certain criteria and making contact with such individuals in advance, is an effective method to ensure robust board and committee succession. Although the CEO should be involved in the work of the committee, they should not be involved in its decision-making processes.

In the oversight function pertaining to executive succession planning, the nomination committee can play a key role in ensuring that the organisation is identifying and supporting high potential individuals. They are also well positioned to support diversity and inclusion policies in the same way.

Sustainability committee

A sustainability committee can help reduce matters on the board's agenda by addressing issues such as integrated corporate reporting and the impact of the organisation on the environment and community (in essence meeting ESG expectations as discussed in [Chapter 18](#)). Since the inclusion of Recommendation 7.4 of the ASX Principles regarding disclosure of material exposure to environmental or social risks,⁸ sustainability reports and integrated reporting have increased, driven largely by the focus on ESG matters. To this end, an increasing number of organisations are forming board committees to assist the board in handling specific matters with high relevance to the business, such as health, safety and wellbeing, environmental and social matters. Sustainability committees assist the board in areas such as:

- establishment of the ESG strategic position and related policies as well as oversight over the governance frameworks which will support the strategy
- compliance with applicable legal and regulatory requirements associated with health, safety, environmental and societal matters (including human rights, modern slavery)
- the preparation of greenhouse gas, sustainability and climate-related disclosures (either mandatory or voluntary) for submission to the relevant regulator and inclusion in the annual report.

The industry and nature of the company's activities will be the most significant influence on the need for such a committee and the nature of the material issues it covers.

Other common committees

A number of other committees often exist and are frequently chaired by directors of the board to provide additional oversight on key risk areas, for example:

⁸ KPMG, International Survey of Corporate Responsibility Reporting 2017, <https://home.kpmg/xx/en/home/insights/2017/10/the-kpmg-survey-of-corporate-responsibility-reporting-2017.html>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

- Health, safety and wellbeing committee – often used in high-risk industries such as mining, petroleum and health, where staff are placed in complex production or service environments.
- Information technology (IT) steering committee – generally in place where there is a significant reliance on information technology, such as call centres, emergency response services and technology service providers.
- Research & development committee – often found where revenue generation is dependent on ongoing research activity, such as in the pharmaceutical and mining industries.

Special purpose committees

Special purpose committees are usually established to consider a specific matter and tend to have a limited life span. Nevertheless, the committee's charter or terms of reference should be approved by the full board and the committee should follow the same operating principles as other board committees.

Special purpose committees are often formed to deal with one-off events including:

- takeovers, mergers, acquisitions or divestments
- major builds, capital projects or system upgrades
- reputation matters
- first-time adoption of significant laws, regulations, industry codes and organisational standards.

Benefits of committees

Board committees can produce a number of benefits, such as:

- allowing directors to use their limited time more efficiently and effectively to do board work
- acting as a filter in summarising complex issues and recommending courses of action

- sending a positive signal to investors that major issues are being dealt with by the company
- allowing independent directors to gain a comprehensive understanding of the business.

The ASX Principles suggest that having separate audit, risk and remuneration committees can be an efficient and effective mechanism to bring the transparency, focus and independent judgement needed in those areas.⁹ Where committees are separated, it is important that there are common members such that information transfers between committees and discussions supporting decisions to be made are well informed.

Unless prohibited by a company's constitution, directors have the power to delegate any of their powers to a committee.¹⁰ Such delegations are documented in the board minutes and also generally set out in the committee charters.

It is imperative that all board committees adopt the same type of systematic planning and processes as the full board, including having:

- a written charter
- an annual agenda
- meeting papers and minutes prepared.

Committees should report regularly to the board through a verbal report by the committee chair and any supporting material from the committee meeting that support the recommendations and/or items for board discussion. Committee papers, detailed reports and/or committee minutes should be made available to all board members, ideally through a digital board portal. Committees should also review their charters and membership at least annually, with any recommend changes reported back to the full board.

⁹ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Commentary to Recommendations 2.1, 4.1 and 8.1

¹⁰ Corporations Act 2001, Section 198D.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Some of the challenges associated with board committees include:

- ensuring that the committee is comprised of directors with the appropriate expertise and resources to provide the full board with high quality advice
- the legal question of whether a higher standard of care will apply to directors, who are vested with the responsibility of investigating particular issues and making recommendations to the full board.

As for the board, committees should seek to gain insights from internal and external stakeholders, to ensure that emerging issues, trends and insights are brought to the committee's discussions.

COMMITTEE CHARTERS

The starting point for any board committee is a formal charter or terms of reference. The charter helps committee members understand their duties and responsibilities and how these can be reconciled with the expectations of the full board and the organisation's stakeholders.

A typical committee charter covers:

- the committee's purpose, responsibilities and duties
- the authority of the committee (including delegations by the board)
- the committee structure and terms of appointment for the chair and members
- meeting requirements and procedures (e.g. frequency of meetings, quorum, voting and minutes)
- access to company personnel and independent external advisers
- members' skills and experience requirements
- board reporting requirements
- committee assessment process.

For an example of an audit committee charter (including further detail on the types of key matters which are typically covered), refer to example [Appendix 3 Audit Committee Charter](#).

Committee charters of listed entities should also be posted on the organisation's website and the key features included in the governance statement in the annual report in accordance with the ASX Principles.

COMMITTEE ANNUAL AGENDA

An annual agenda provides the framework to manage the committee's time, resources, meeting frequency and the matters considered by the committee.

An effective annual agenda:

- reflects a complete picture of the committee's roles and responsibilities
- is aligned with the board annual agenda to ensure integration of the board and its committees
- provides a summary of the committee's key activities
- prevents meetings being 'crowded out' by peripheral issues
- ensures the committee's insights and expertise are fully utilised.

The annual agenda brings the committee charter to 'life' as it drives the committee's:

- activities
- meeting agendas
- information requirements.

For more information, refer to the example audit committee annual agenda set out in [Appendix 5 Audit Committee Annual Agenda](#).

Discussion on the annual agenda solicits the involvement of committee members concerning the nature and timing of agenda topics. The committee's annual agenda also helps to determine non-committee members who should be invited (including management and external advisers) to meetings and identifies potential conflicts of interest.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

COMMITTEE INDUCTION FRAMEWORK

All committees have significant responsibilities. It is not sufficient for committee members to have only a rudimentary knowledge of the specific matters under consideration. Committees cannot provide meaningful protection for shareholders unless their committee members are in a position to challenge management. To do this effectively, they must have the skills, knowledge and expertise, and be supported by access to independent advisers. A formal induction framework for new committee members is essential. Induction should comprise the provision of an information package with key business documentation, training sessions and meetings with key business executives. [Appendix 4 Audit Committee Induction Framework](#) provides details on what should be included in the audit committee induction framework which can be leveraged for other committees too.

COMMITTEE MEETING AGENDA AND MINUTES

Each committee meeting agenda should be prepared with reference to the committee's charter and annual agenda. The committee chair and company secretary should take responsibility for the content of the agenda, seeking input from committee members, the CEO and senior management, where practicable.

The process of setting the agenda should involve:

- consideration of content
- ordering of items
- allocation of time for each item
- deciding on invitees.

Careful preparation of the agenda will enhance the committee's productivity by focusing the committee's attention on the critical matters requiring examination and discussion. Committee minutes must be a complete and accurate record of the resolutions adopted and recommendations made by a committee, evidencing that the committee has acted with due care.

The company secretary, or delegate, is responsible for maintaining a complete set of committee papers, including minutes of meetings, meeting agendas and supporting papers.

Committee draft minutes should be circulated to members after meetings and to all directors for information as soon as possible after the meeting (KPMG suggests that good practice is to do this within 14 days).

Approval of minutes should coincide with the next meeting of the committee.

COMMITTEE SIZE AND COMPOSITION

While the size of a committee varies according to the organisation, a sufficient number of members with the necessary knowledge and expertise should be present in any committee. Notwithstanding the minimum of three members recommended by the ASX,¹¹ KPMG suggests that for large organisations, committees should be made up of at least four members to allow sufficient diversity of skills and experience as well as enabling the committee to function effectively in the event that one member is unable to attend a meeting.

In determining the appropriate size for each committee, the board should take into account the:

- complexity and geographic diversity of the organisation
- nature and extent of its responsibilities
- knowledge and experience required of committee members
- minimum number of members to allow a workable quorum
- numbers needed to encourage robust and insightful debate.

¹¹ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The ASX Principles indicate that the audit, nomination and remuneration committees should:

- consist of a majority of independent directors (and in the case of the audit committee, should consist only of non-executive directors and be chaired by an independent director (who must not be chair of the board))
- have at least three members.¹²

Committees usually deal with technical matters, such as financial reporting standards, risk management and executive remuneration. Therefore, ensuring committee members have the relevant skills and experience, as well as access to expert advice, is paramount.

Where allowed for in the Constitution, committees can include independent members who are neither members of the executive nor members of the board.¹³ Bringing in external expertise in this way gives the committee access to relevant specialist knowledge and can also be a useful tool to support director succession. The following considerations are important where external advisers are included in committees:

- **Committee charters** should clearly define the roles, responsibilities, and voting rights of external members.
- External members typically serve in a **non-voting advisory capacity**, unless formally appointed as directors.
- **Conflicts of interest**, confidentiality, and fiduciary duties must be carefully managed.

¹² ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendations 4.1, 2.1 and 8.1 and Commentary.

¹³ Section 198D of the Corporations Act 2001 (Cth)

COMMITTEE/BOARD INTERACTION AND REPORTING

Board committees are an effective forum for investigating and reviewing important issues in more detail than the full board's agenda normally allows for.

The board should expect the reports it receives from its committees will be:

- complete, but concise
- timely
- accurate
- compiled with integrity.

Whilst the committee may complete background work and make recommendations to the board, or act where the delegation to the committee permits, the overall responsibility for decisions always remains with the full board.

It is, therefore, essential for directors to:

- question the committee chair and members when the committee report is being presented
- not blindly rely on any information or advice provided (even 'expert' recommendations)
- challenge whether the organisation's culture is appropriate, including the 'tone at the top', from a control perspective
- be informed of any issues on which committee members were not in total agreement
- confirm that any external parties (e.g. auditors) have been effective in providing the required assurance.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

COMMITTEE EVALUATION

Board committees, like their parent boards, should be evaluated on a regular basis to improve their effectiveness and typically committees are evaluated at the same time that the board evaluation is completed. Disclosure of the process of evaluating the performance of both the board and its committees is recommended by the ASX Principles.¹⁴

The focus of the evaluation assessment should include looking at the committee's:

- structure, role clarity and authority
- composition, skillsets and development
- leadership, relationships and processes
- nature and scope of work.

A typical assessment process includes:

- a self-assessment survey
- interviews with committee members, management and assurance providers as well as other directors (so as to understand how the board views the committee's performance)
- a review of the quality, quantity and relevance of information coming to, and emanating from, the committee.

The assessment's outcome should be a report providing an objective, balanced evaluation of the committee's effectiveness, highlighting specific areas for improvement.

As a good governance measure, committee evaluations should be performed on an annual basis (even if only informal). Individual assessments of committee chairs should be undertaken regularly by the chair of the board, and by the committee chair for individual committee members.

For further information please contact:



Caron Sugars

**Lead Partner,
Board Advisory Services
KPMG Australia
ccobargsugar@kpmg.com.au**

¹⁴ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendations 1.6.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

12. Investment Management

Entities such as asset and wealth managers (superannuation funds, investment managers and banks), insurers, health funds and organisations which invest funds to meet both short- and long-term obligations, have the task of prudently investing funds whilst balancing the need to obtain a reasonable return with managing the portfolio so that it operates within the agreed risk appetite and tolerance.

This must be achieved within a robust risk and reporting framework to achieve compliance with applicable regulatory requirements.

In this chapter

- The role of the board
- Investment committees
- Investment framework
- Risk appetite
- Risk tolerance
- Investment strategy
- Asset allocation
- Financial risk management
- Investment policy
- Investment performance and risk management reporting
- Outsourcing – fund managers and external providers

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Are directors convinced that the board/organisation's risk appetite is aligned with management's risk appetite for each investment/financial risk?
2. Does the investment policy make sense intuitively, including articulating the rationale for a particular investment strategy?
3. Do the investment mandates given to service providers, such as fund managers, align to the investment policy?
4. Is there a process to monitor compliance with the investment policy – including by outsourced service providers?
5. Is the investment selection process documented and undertaken by appropriately qualified investment management staff?
6. Would it be useful to employ an external specialist adviser to provide advice on asset allocation strategies?
7. Is there separation of duties between the custodian, fund manager and asset consultant (e.g. it is preferable for the asset consultant not to be providing investment products)?
8. Is investment management performance regularly reviewed and critically examined?
9. Is investment management performance exceeding index-based performance – because if it is not – then why is the organisation paying additional fees for 'active management'?
10. Are investment management fees and custodian fees regularly reviewed and periodically tested to the market?
11. What information is available in relation to investment risk (e.g. investment risk ratios, value at risk, stress testing, counterparty risk)?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- Lack of a formal, documented and comprehensible investment policy. It should be easily understood by a competent, but non-technical director.
- There is not an investment strategy directing the investment activities.
- The investment policy and strategy have not been reviewed for over three years and one year respectively.
- An investment performance benchmark is either deemed not appropriate, not established, or not aligned with the risk appetite.
- The performance of external managers is not measured or reviewed.
- There appears to be inadequate segregation of duties, inadequate controls and breach reporting is either not formalised or is inadequate.
- There are large variances in reported performance over periods.
- There is a lack of independent verification of performance or compliance with the investment policy.
- Non-compliance with investment policy – which may be consistent in nature or not be detected in a timely manner.
- Management is very defensive when asked logical questions or becomes aggressive towards third parties, such as auditors, when reasonably challenged.
- There is a high dependence on one key individual in terms of the management of funds.
- There is confusion at the investment committee in terms of interpreting various reports or advice received from parties, such as an asset consultant.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

This chapter of the Director's Toolkit provides guidance to directors who are responsible for overseeing investment governance, operations and processes. Due to the need for brevity, as well as the complexity of various regulatory environments, this chapter covers the general issues associated with better practice investment governance, rather than specific regulatory requirements. Further references that provide more detail are provided at the end of the chapter.

THE ROLE OF THE BOARD

Ultimately the board is responsible for investment management, including the overall investment beliefs and philosophy, the investment strategy, investment policy and associated risk appetite and tolerance.

Even though the board may delegate these responsibilities, either in whole or in part, to a board committee, such as the Investment committee, or rely on the advice of an asset consultant, the board is still ultimately responsible for investment management.

INVESTMENT COMMITTEES

The investment committee traditionally tends to be a board committee, rather than a management committee, and is responsible for the investment strategy, as delegated by the board. The investment committee would also be responsible for the monitoring of investment performance and either approving investment decisions or recommending investment strategies to the board in line with its charter and delegations. Further details regarding board committee composition and structures are provided in [Chapter 11](#).

INVESTMENT FRAMEWORK

The investment framework supports the organisation's process for formulating an investment strategy. An investment framework includes the governance, policies, systems, processes and people to operate and oversee the management of investments, including the management of the investment and financial risks.

RISK APPETITE

The collective risk appetite of the organisation is a key determinant in the construction of the investment portfolio. It is important that the risk appetite of the board and management are aligned (which is often not the case) and, ultimately, it is the board's risk appetite which is paramount.

Risk appetite is driven by a number of factors, including:

- the values of the organisation and the types of investments it is, and is not, willing to make
- the amount of funds available for investment (i.e. the greater the amount the more diverse and sophisticated the investment choices)
- the period of time over which funds are available (i.e. generally, short term equates to a lower risk, longer term enables greater risk; exceptions to this include long-term bank deposits where the longer term risk is generally low)
- what the uses for the funds are (e.g. capital expenditure, supporting financial liabilities) and when that use is required or forecasted to be required
- the ability to withstand volatility in the investment portfolio (i.e. less than one in X years chance of negative returns)
- capital requirements (i.e. for insurance companies, higher risk investments require higher levels of capital)
- the complexity of investments
- the capability and experience of the investment framework, including personnel
- the requirement to make regular dividends/distributions to share/unit holders
- restrictions on certain types of asset class, based on ethical, social or environmental risks (e.g. the tobacco industry)
- investment diversity guidelines for the portfolio, including minimum credit ratings of investment counterparties.

Once the risk appetite has been agreed then the investment selection/asset allocation process can commence.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

RISK TOLERANCE

Risk tolerance sits hand in glove with the risk appetite of the organisation. Risk appetite focuses on defining the boundaries within which investments are made. It is a higher-level statement that defines the amount of risk the organisation is willing to take in order to meet its investment objectives. Risk tolerance is the degree of volatility that the organisation is willing to accept within the parameters of its risk appetite.

For example, an organisation's risk appetite statement may state that it does not accept risks that could result in a 'significant loss in revenue'. A risk tolerance statement would then go on to define the specific levels of acceptable variation within that risk (e.g. the organisation may only accept a 10 percent loss in revenue from a particular asset class in any given period; for example, a year).

The questions to consider in the development of the organisation's risk tolerance statement are, therefore, inherently linked to those used to develop the risk appetite.

INVESTMENT STRATEGY

The investment strategy is the key document defining the strategic investment objectives, and the guiding framework and principles determined by the board to be appropriate for the organisation's broader operating strategy. Its key components include:

- Investment purpose and the alignment of organisational values to the investment strategy (e.g. 'ethical' investment principles).
- Asset allocation principles – such as how the portfolio will be constructed in order to meet the desired risk/return outcome.
- Risk management guidelines – including clear risk appetite and risk tolerance targets.
- High-level policy statements – including the monitoring framework that details what will be monitored and the specific measures in place to track performance.

ASSET ALLOCATION

To implement the investment strategy, the organisation should have an asset allocation process in place which includes robust due diligence. Asset allocation involves dividing an investment portfolio among different asset categories/classes. This is a crucial step to ensure that investments selected are aligned to the organisation's investment objectives, including risk appetite and tolerance.

The due diligence process should consider historical returns for particular asset classes and the volatility of return/value of the instrument (i.e. risk) over various time periods. Considering these factors can be insightful and assist in identifying correlations between assets, while helping to dispel common preconceptions about various assets. For example, some assets may be considered to have low returns, but when looked at over the long term, they perform well with low volatility, providing a form of capital protection.

Another relevant example in asset allocation is where funds are needed in the short term and a loss cannot be tolerated. Therefore, the logical asset allocation would be to defensive assets such as cash, term deposits and short dated fixed interest securities, all of which impacts the return that can be achieved.

Many research and academic articles indicate that asset allocation is a key driver of returns, rather than stock or security selection – hence the importance of having a robust framework and process in place to determine asset allocation.

Having allocated assets, an organisation should also have arrangements in place for the ongoing management and monitoring of its investment strategy. Depending upon the value of funds invested, this may include asset allocation rebalancing processes, exposure management arrangements (i.e. derivatives and currency), investment transition arrangements, processes to monitor investments and valuation procedures. It is critical that the reporting framework to monitor investments provides directors with meaningful information in a timely manner.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

FINANCIAL RISK MANAGEMENT

When directors are overseeing the investment process, they need to be mindful of the financial risks associated with the investment process and not just the asset allocation decision.

A robust risk management framework needs to be established and implemented to address the risks arising from the investment of funds. These risks would include:

- liquidity risk (ensuring that investments can be readily converted to cash, if required, without suffering a significant loss or that sufficient cash is held as part of the investment portfolio)
- credit risk (the risk of loss resulting from counterparty default)
- market risk (the risk of loss in value of investments due to the adverse effects of movements in interest rates, equity prices, foreign exchange rates, commodity prices, etc.)
- operational risk (the risk of loss resulting from errors in the processing of transactions, a breakdown in the control environment or errors or failures in systems)
- reputational risk (the risk of damage to the reputation of the organisation due to the nature of the investment or loss in value of the investment – particularly important for government and widely owned organisations)
- environmental, social and governance (ESG) risk (the risks associated with failing to meet ethical, social and environmental expectations that generate a loss of business value through stakeholder activism, and perceptions of the organisation's misalignment of its business to the broader societal values. In addition, ensuring the appropriate approach is taken to govern the risk management decisions and activities).

Financial risk management arrangements would typically comprise a range of tools for risk measurement and analysis that are commensurate with the investments of the organisation. One very good example of this is the use of stress testing and scenario analysis, which can assist the organisation to identify and assess potential risk exposures that may threaten the likelihood of achieving investment objectives. Stress testing should be a forward-looking assessment of possible risk factors. Importantly, the outputs from stress testing should enable directors to make informed decisions on the management of the portfolio to enhance returns and reduce financial risk.

INVESTMENT POLICY

Having determined the investment beliefs and philosophy, objectives, strategy, risk appetite, risk tolerance and approach to financial risk management, it is important that this is documented in the investment policy.

The fundamental importance of an investment policy is that it provides the framework for an organisation to achieve its investment objectives (as defined in the investment strategy) and seeks to avoid unacceptable outcomes. The policy ensures that the risk appetite and philosophy of the organisation are reflected in its investment activities.

The purpose of the policy is to provide general guidance regarding the investment objectives, specific guidance on strategies to achieve the investment objectives, and to provide a mechanism to control management behaviour and reduce bias and potential errors arising from decision-making.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

An investment policy should address the key areas of:

- the investment objectives, philosophy, risk appetite and risk tolerance, including an explicit mandate for values-led/ethical investment strategies (e.g. addressing ESG including, for example, not investing in gaming/tobacco)
- the asset allocation strategy and the rationale by which those objectives are to be pursued
- guidelines on investment exposures and maturity periods
- guidelines on counterparty exposure limits
- liquidity requirements
- the mandates with which underlying investments must comply and, in the case of pooled investments, the guidelines in place for the selection and contracting of managers and how they align to the organisation's investment mandate
- any socially responsible investments and prohibited investments
- the benchmarks against which the performance of investments and managers are to be assessed
- the valuation approach and methodology for unlisted or illiquid investments
- the methodology for deciding and disclosing proxy voting decisions
- the reporting required to be provided to the investment committee and the board
- the responsibilities of various stakeholders, including the board, investment committee and management.



Case study: ethical investment

In February 2014, Transfield Services (Transfield) made a commercial decision to broaden its services and invest in the management of detention centres. With large government contracts on offer for the management of controversial detention centres, both in Australia and offshore, the Transfield board saw the potential for large, stable returns. These contracts eventually were estimated to contribute up to 15–20 percent of the company's revenue (in the wake of lost revenue from the declining resources sector), and saw an increase in Transfield stock price of up to 140 percent.

However, only 18 months after the investment decision, Transfield were facing a major issue, with many of its shareholders withdrawing their investment in Transfield due to claims of abuse within the detention centres. Under the confidentiality clauses of the Government contracts, the company was unable to answer questions from investors about the abuse claims, making it difficult to transparently disclose how the company undertook the operation of the centres.

As a result of the perceived lack of transparency, together with the instigation of Senate hearings to investigate the claims on the back of public and political pressure, Transfield stock dropped in value by 45 percent.

Whilst commercially, the investment decision was sound, aligned with the board's investment metrics and had a short-term positive impact on shareholder value, ultimately, a lack of consideration of social, political and contractual drivers undermined the return and potentially caused significant financial and reputational damage through divestment of Transfield stock by key shareholders.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

INVESTMENT PERFORMANCE AND RISK MANAGEMENT REPORTING

Having executed the investment strategy, the investment performance and risk management reporting will need to be undertaken to measure the performance of investment activities against the investment objectives and benchmarks. At a detailed level, this will involve comparing the performance of investments and managers to agreed benchmark indices. Other considerations include:

- frequency (usually a minimum of monthly reporting for management)
- documentation – the reporting process should be documented in procedures
- detail/content (e.g. manager performance, compliance, portfolio values, credit risk and other risks)
- format, such as the use of an 'Investment Report Dashboard'
- distribution (i.e. executive management, middle office/compliance function, investment committee, etc.).

OUTSOURCING – FUND MANAGERS AND EXTERNAL PROVIDERS

Depending upon the size of the funds available for investment, the outsourcing of various activities may be appropriate. This could include the outsourcing of investment activity to fund managers, the use of asset consultants to determine asset allocation and the use of a custodian for the settlement and recording of investment transactions. However, there are also risks arising from the outsourcing of activities which need to be recognised and managed.

Outsourcing and the use of external providers should also take into account:

- the benefits of outsourced investment management given the capabilities of in-house staff and the complexity of investments
- the nature of asset classes invested in
- the scale and size of investments
- system requirements to support outsourced arrangements
- the use of index funds versus active investment manager funds
- external manager assessment, selection and monitoring processes
- the custody and investment administration requirements.

It is also important that the 'mandates' given to investment service providers, particularly fund managers, are consistent with the investment policy. It is not uncommon for an investment policy to prohibit the use of derivatives, only to find a fund manager using derivatives – because it is not prohibited in the mandate provided to the fund manager.

Critically, an organisation can outsource its investment activities, however, it cannot outsource its legal accountabilities and responsibilities. Directors and investment committee members should also consider APRA's prudential standard SPS 231 in relation to outsourcing for more specific guidance.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- Certain industries such as superannuation, health and insurance are subject to various regulatory requirements relating to the management of investment funds. For example, superannuation funds and insurance entities are regulated by APRA and ASIC, and health entities are regulated by APRA.
- The regulation of these industries also provides guidance for other organisations. For example, on the topic of investment governance, APRA has released a prudential standard (SPS 530) and related guidance notes (SPG 530).
- Australian Prudential Regulatory Authority (APRA), <http://www.apra.gov.au>

For further information please contact:

**Sean Comerford**

Partner, Consulting
KPMG Australia
scomerford@kpmg.com.au



FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

13. Productive Meetings

Meetings of directors should be forums of informed discussion and decisions – not an endless stream of surprises.

In this chapter

- Duties related to board and committee meetings
- Meeting papers
- Meeting procedures
- Decision-making process
- Decision-making outside the boardroom
- In camera sessions
- Boardroom conduct
- Technology
- Confidentiality
- Independent professional advice
- Board minutes
- Meeting evaluation

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Is the number and length of board meetings sufficient to allow the board to effectively discharge its duties and responsibilities?
2. Are board members able to access the previous meeting's board minutes with ease and review these prior to the next board meeting?
3. Are all board members provided sufficient time to review the board papers prior to entering the meeting?
4. Is the chair clearly accountable for the agenda's content, with all directors and committee chairs having the opportunity to contribute?
5. Does the board agenda allow sufficient time for strategic discussion?
6. Are in camera sessions used appropriately to focus the board on what is required from them and any key concerns?
7. Are communication channels used by the board to conduct its business secure and confidential?
8. Is the size of the meeting group appropriate, having regard to the purpose of the meeting, and are all attendees directly relevant?
9. Is regular feedback and evaluation of the effectiveness of meetings provided to board members?
10. Does the board manage actions arising from board minutes, with outstanding actions being reviewed at each board meeting?
11. Is the board undertaking critical and regular assessment to identify opportunities for improvement?
12. Has the board allowed sufficient time for committee reporting such that they are satisfied delegated authorities are being executed appropriately?
13. Has the constitution been reviewed to ensure that any clauses regarding form of resolutions (digital vs physical), signature requirements (ink vs digital) and use of technology enable digital signing and circular resolutions?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- Board or subcommittee meetings are not scheduled on a regular basis.
- Meetings are held too frequently, resulting in a greater focus on operational issues as directors get into BAU activities rather than taking a more strategic posture over organisational performance.
- Meeting agendas and materials are sent out with little time for review or director contribution.
- Board members do not read board papers prior to attending the meeting.
- Board papers are voluminous and don't provide the appropriate insights and analysis to facilitate discussion on key agenda items.
- Board papers are regularly changed at the last minute.
- The company secretary provides incomplete or delayed distribution of board meeting minutes after meetings.
- Directors attend less than 50–75 percent of meetings held (depending on the nature of the organisation).
- Many issues discussed carry over to the next meeting.
- Attendee and absentee lists are kept irregularly and sometimes are not noted in the minutes.
- There is no information sharing portal set up for the board, and directors rely on emails and handouts to communicate and store information.
- Often meetings are closed without an agreed set of actions.
- There are very few or no non-executive director/'in camera' sessions.
- At the end of each meeting a review of the effectiveness of that meeting is not undertaken before closing.
- Meetings are being recorded without the board's knowledge and/or with their knowledge but without a policy stipulating how and when this can occur and how recordings should be managed.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

DUTIES RELATED TO BOARD AND COMMITTEE MEETINGS

Directors are expected to prepare for, attend and contribute meaningfully to board meetings in order to discharge their director duties. A director's meeting attendance record is often taken into consideration by proxy advisers when determining whether to make a recommendation to shareholders supporting a director's re-election to the board.

Unless the company's constitution provides otherwise, the quorum for a directors' meeting is two directors, and the quorum must be present at all times during the meeting.¹

Boards need to be aware of the requirements relating to the conduct of board meetings imposed by formal documents such as the board charter and company constitution.

Chair

The chair plays a central role in the effective functioning of meetings, maintaining responsibility for leadership of the board and its efficient organisation and functioning. The chair is responsible for setting the board agenda and ensuring adequate time is available for discussion of all items. It is important that the chair leads and facilitates discussions, encourages the participation of other members, ensures that all directors have a say, and conducts meetings in an effective manner.² The chair must ensure the board's time is used to focus on the most important issues and that the discussion is open, collegiate and relevant to the agenda items.

The role of a strong chair includes encouraging all directors to:

- identify and challenge their biases
- engage in active debate
- listen to internal alarm bells and give them a voice
- have the courage to speak up
- challenge management, where appropriate
- not to back away when a difficult issue arises
- promote clarity of purpose.

¹ Corporations Act 2001, Section 248F.

² Australian National Audit Office, Public Sector Audit Committees: Independent Assurance and Advice for Chief Executives and Boards, August 2011.

Company secretary

The company secretary is instrumental in ensuring meetings run smoothly. An efficient company secretary is proactive and will anticipate the needs of directors.

With respect to board meetings, the company secretary should ensure:

- the board agenda and briefing materials are completed and distributed in a timely manner
- appropriate personnel have been invited to the meeting
- presentations are concise and highlight significant issues
- the chair is appropriately briefed and supported
- the meeting venue and location is appropriate and secure
- audiovisual and other equipment is operational
- expert advice is available when required.

In boards where no company secretary exists, these duties often reside with management and the chair. Many organisations appoint administrative staff members to assist with the preparation and distribution of board documents, however, the responsibility for ensuring that this occurs remains with the chair.

Board committees

Board committees provide an effective way of distributing work between directors and allow for more detailed consideration of important issues than would be possible during scheduled board meetings. Committees allow directors sufficient opportunity to focus on relevant matters without having to compromise the limited time available during full board meetings. Committee meetings should apply the same governance protocols as those described in this chapter for board meetings.³

³ See Chapter 11 (Board committees) for a further discussion of board committees.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Meeting attendance

As a part of their duties and responsibilities, directors should be present for board and appropriate committee meetings. Absenteeism will never excuse a director from their duties to the company. To facilitate participation, directors may attend in person, or virtually.

Directors who are unable to attend a meeting should ensure their apology is given in advance and noted in the minutes. In the case of public companies, attendance is measured and documented in the annual directors' report. If there are repeated absences on the part of a director, the chair may need to meet with the director to ascertain their future availability and commitment. In some circumstances it may be in the company's interest for the director to resign.

To facilitate the effective conduct of the meeting, it is important to:

- establish and circulate a clear and appropriately detailed agenda in advance
- consult with any independent advisers or members of management whose participation is required, and limit attendance at board or board committee meetings to the extent necessary
- establish an appropriate meeting environment (including style, location, room size and seating)
- ensure the meeting begins and ends promptly at the scheduled times
- be aware of particular customs, rules and etiquette for the meeting.

Members of management are often invited to meetings to present papers and engage with the board on matters for broader discussion. The inclusion of management in board meetings can be a helpful way to generate transparency and build trust between the executive team and the board. However, having too many people attending and/or observing in this way, can impact on decision-making efficiency as well as increase the risk for breaches of confidentiality.

Meeting frequency and duration

The Corporations Act does not prescribe the number of directors' meetings that must be convened. Both the frequency and duration of meetings are factors which influence the quality of board output. The board must agree on the frequency and duration of meetings required for it to effectively address all matters listed in its annual agenda.

In Australia, boards previously held monthly meetings. However, there is a growing trend suggesting that longer duration bimonthly meetings, in addition to specific strategy meetings, may be more effective. As the business environment is constantly evolving, and information and issues arise more quickly, the more traditional frequency and structure of meetings may also need to be reconsidered. Board agility is an important factor in enabling issues to be considered when they arise, rather than waiting for the next board meeting. In these instances, mechanisms for formally considering board matters can be leveraged, such as meeting virtually for an ad hoc meeting or circular resolutions.

Public companies are required to include in their annual report the number of board and committee meetings held each year and the attendance of each director at these meetings.⁴

The length of the meeting should be sufficient to give appropriate attention to all issues at hand. When planning the agenda for a long meeting, it may be useful to consider whether splitting the meeting into two shorter meetings would be more appropriate. If the meeting must be kept to a single session, scheduling breaks is vital to keep participants focused, attentive and productive.

A meeting should only be held if it is necessary. If the same information could be covered in an email or report, for example where all agenda items are information sharing, a meeting should be avoided. As meetings are costly, the outcome must be valuable enough to justify holding the meeting.

The replaceable rules in the Corporations Act provide that a director can call a directors' meeting by giving reasonable notice to every other director.⁵

⁴ Corporations Act 2001, Sections 300(10)(b) and 300(10)(c).

⁵ Corporations Act 2001, Section 248C.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

It is crucial that board members have sufficient notice of forthcoming meetings. Circulation of a list of prearranged dates is sufficient notice and typically a convenient practice. Given time pressures on directors, some companies prearrange meeting dates two years in advance to have these times locked into diaries.

Meeting preparation

Careful preparation of the agenda enhances the board's productivity and supports its strategic and oversight role. The board meeting should be an opportunity for directors to add value to the discussion and not be informed on the issues for the first time.

The purpose of the meeting should be communicated amongst members in advance, allowing sufficient time to become familiar with the proposed agenda and undertake any research required. In order for a meeting to be productive, a strategically defined purpose should be linked to specific plans and outcomes.

The chair must also review the board papers prior to any meeting to identify any potential conflicts of interests for board members and raise these with the individual prior to the meeting. This relies on ongoing, open dialogue between the chair and other board members regarding potential conflicts of interest.

Agenda

A board meeting agenda enables directors to be fully informed of issues to be proposed and discussed at the meeting, reducing the time required on briefing at the beginning of a meeting. It should be referenced to the annual agenda, which identifies matters to be periodically included on the board agenda.

The chair, working with the company secretary, should be accountable for the agenda's content. Input should be sought from directors, the CEO and senior management, and the chairs of board committees. Setting the agenda should involve consideration of content, the ordering of items, the allocation of time for each item and deciding on invitees. High-priority items should be scheduled first and it is essential to clarify which items are for decision (resolution), discussion, noting or information purposes. A timed agenda will assist directors in recognising the relative significance of each issue and ensure the meeting finishes on time.

Agendas drive the direction and focus of board matters. It is therefore important that they are well thought through and structure the meeting to allow for the appropriate balance between compliance driven matters and strategic discussions.

Typically an agenda should clearly include:

- Time for ensuring a quorum is present
- Declaration of any conflicts of interest
- Approval of prior meeting minutes and a review of outstanding action items
- Standing reports from CEO and or Board sub-committees
- Strategic discussion items
- Decision and action items
- Items for noting
- Governance matters (such as board evaluations, policy reviews)
- In-camera session
- Any other business
- Future meeting dates

To enable good time keeping and indicate the expected level of discussion for each agenda item, the start and finish times for each item (or minutes allowed) should be included on the agenda.

Consent agendas

Often Boards have a lot of matters to address in a limited time, leading to an increase in the use of mechanisms like 'consent agendas' to streamline the noting and endorsement of items that are routine, non-controversial or do not require discussion. The approach allows the Board to approve these items in one motion rather than individually.

When using a consent agenda approach, the chair must provide directors with an opportunity to take any item/s off the consent agenda to allow for discussion during the meeting.

In practice, items to be included in the consent agenda are circulated as part of the pre-meeting papers. This gives directors an opportunity to review the items and determine whether there are any matters that they would like to bring to the group for discussion.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

For a consent agenda to work effectively, directors must be clear on which matters are included as consent agenda items. Directors must also commit to reviewing materials beforehand and therefore requires disciplined preparation and communication.

Whilst consent agendas can improve the efficiency of meetings, it is important to regularly review the items included to ensure that the process is functioning as intended.

MEETING PAPERS

Review of papers prior to the board meeting

Board meetings are a place for discussion and decision-making. To make effective use of the often limited time available, all board papers should be read prior to the meeting, with questions and comments noted and ready to be raised. A well-functioning board will distribute a complete set of board papers at least one week prior to the meeting. This pack will include:

- An agenda with all items for discussion, noting and decision clearly noted, together with the timing allocated for each item (as in indication of importance).
- A copy of the prior meeting minutes for approval.
- A list of outstanding action items.
- Copies of any committee reports being tabled.
- Copies of all regular reports (e.g. financial reports, performance reports, compliance reports and risk reports). These should be in a consistent, succinct and clear format with content that directly aligns to the organisation's strategic and operational KPIs; and relevant information to support specific agenda items.

Many boards describe being inundated with volumes of reading prior to board meetings, making it almost impossible for directors to do the required pre-reading and adequately digest and consider the relevant information. High volumes of board papers are symptomatic of:

- Management being unaware of what information the board requires. If there is no clarity regarding matters requiring board consideration, issues that need to be escalated or how the

information requested relates to strategic objectives and KPIs, there is a tendency for management to 'give them everything' in the hope of meeting expectations.

- Management attempting to overwhelm the board with irrelevant information in the hope of distracting time and discussion away from known problem areas.
- The board being unable to articulate to management the key information that they need to support their decision-making processes. Directors and boards that request large amounts of supporting data can often be lacking clarity in direction or confidence in their decision-making.

In each scenario, it is up to the board to set the criteria and basis of information to be provided. Board papers should strike an appropriate balance between quality and quantity, and should be concise documents that fully present the information the board will require to comprehend all issues and make appropriately informed decisions (where a decision is required). They should be prepared to strict standards in terms of presentation and content, share a consistent format and include the date, version reference, author and reviewer's name and title. The purpose of each paper should also be clearly indicated. Directors should establish clear criteria for what matters should be raised at board level and why. Once that has been established, directors should then be willing to challenge the quantity and quality of papers provided by management. Poor papers are a major cause of bad board decision-making and create a difficulty in reaching a consensus.

The content of papers should reflect the following comments provided in section 3.1.3 of the Hayne Final Report:⁶

'Boards must have the right information in order to discharge their functions ... When I refer to boards having the *right* information, I am not referring to boards having *more* information. As I noted earlier, it is the quality, not the quantity, of information that must increase. Often, improving the *quality* of information given to boards will require giving directors *less* material and more information.'

⁶ Final Report, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, p 400

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Access to meeting papers

Technology is rapidly moving into boardrooms, with the digital distribution and hosting of board papers commonplace. Electronic communication methods facilitates the exchange of timely and accurate information between board members however, the adequacy of the security of data sharing and storage technology should be carefully considered when exchanging highly sensitive and confidential company information.

Electronic portals are commonly used by boards to securely post and retain materials, including board minutes, policy documents, agendas and other core documentation. Further uses include providing updates on the activities of board committees, enabling real-time communication and collaboration between board members, and facilitating information sharing between directors and management.

The way in which directors access such information has changed too. Most boardrooms now have board members using a digital device (tablet or laptop) and accessing the portal for board documentation in the meeting. Digital devices which include authentication controls and encryption offer a considerable security improvement over traditional hard copy distribution. However, professional advice may be warranted regarding security and document retention concerns where information is downloaded from portals, or saved from emails, onto personal devices.

MEETING PROCEDURES

It is the role of the chair to ensure that meetings are run to time and that all matters are discussed and actioned appropriately. It is the responsibility of directors to ensure that they work with the chair to achieve these objectives.

DECISION-MAKING PROCESS

The emphasis in the boardroom is on consensus decision-making, which focuses on securing the agreement of the full board. If unable to reach a consensus, the board should state the reasons for this and endeavour to solve the issues or find further information required to make a decision.

The board and management should agree on having a number of predetermined elements included in all material proposals for board decision. It is important these elements are seen as guidance, and that management exercises common sense and business acumen in deciding what information to provide to the board.

The following elements at a minimum should be considered in material proposals for informed decision-making:

- alignment with strategic direction
- values and behaviours
- financial and reputational impact and considerations
- economic and financial assumptions
- key risks and dependencies
- legal and regulatory obligations
- availability of resources (internal and/or external)
- ethical and environmental dimensions (e.g. directors should consider 'should we', not just 'can we')
- shareholder and stakeholder perspectives
- description of due diligence completed
- benefits or outcomes are measurable and can later be tested
- contingencies to deal with unexpected developments
- monitoring and accountability mechanisms – in particular, are actions being addressed in a timely manner.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

DECISION-MAKING OUTSIDE THE BOARDROOM

In some situations, decisions need to be taken before the next scheduled directors' meeting. It is usually permissible to circulate a resolution for approval by directors without the need to convene a meeting, though this process should be reserved for urgent matters or more procedural matters. Unless the company's constitution provides otherwise, the resolution must be signed by all directors entitled to vote on the matter and it is deemed as being passed when the last director has signed.⁷ Even so, best practice requires that a written resolution of the directors is passed unanimously (that is, it must be signed by all directors and not just a majority), as a written resolution of directors does not otherwise provide an adequate forum for further discussion on the issues at hand should one or more directors be inclined to vote against the resolution. Separate copies of the document may be used for signing, provided the wording of the resolution and statement is identical in each copy.⁸

Contemporary governance practice supports the use of:

- Scanned signatures
- Email confirmations
- Board portal voting
- Electronic signature platforms (e.g., DocuSign)

But these methods are only valid if permitted by the company constitution. If the constitution is silent or restrictive, physical signatures may still be required.

There are some matters for which a rotary/circulating resolution is not permissible, for example where the directors make a declaration of solvency prior to a voluntary winding up. Here, there is a requirement that directors have formed an opinion on solvency at 'a meeting of directors'⁹ (which could be held virtually). Typically, most matters are best dealt with at a directors' meeting where appropriate discussion can take place.

Once the resolution has been passed, it must be entered into the minute book and noted at the next meeting of directors.

⁷ Corporations Act 2001, Section 248A.
⁸ Corporations Act 2001, Section 248A(2).
⁹ Corporations Act 2001, Section 494.

IN CAMERA SESSIONS

Non-executive directors should consider the benefits of meeting without the presence of management. These meetings are known as 'in camera' sessions, and can be held when non-executive directors consider it appropriate to convene without the presence of the other directors and management. Most often this is at the start or the end of each board meeting, to allow free-flowing and candid discussion. Directors tend to find that having the in camera session as standard on the agenda any angst from management about the practice. Further, starting each meeting with an in camera session allows the chair to identify any key concerns that directors may be seeking to gain an understanding of in the board meeting.

The types of subjects that could be usefully discussed at an in camera session include:

- CEO performance and remuneration
- relationships between directors
- relationships with management and assurance providers
- director performance issues
- 'tone at the top' concerns
- whistleblower issues relating to senior management
- confidentiality issues
- potential conflicts of interest
- independence concerns relating to assurance providers
- sensitive matters affecting management and/or assurance providers.

Whether there should be minutes of an 'in camera' meeting is up to the board and will depend on the nature of the discussion. Some organisations allow their minutes to simply state that an 'in camera' meeting took place, while others may be more descriptive. Any formal actions that arise from an 'in camera' session should be documented, allowing outcomes to be tracked in subsequent meetings.

In-camera meetings are also typically held regularly with the internal and external auditors to enable questions of governance and culture to be asked without management present. This should be included on the agenda to ensure that the meetings occur.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

While the company secretary plays a vital role in governance, their attendance at in camera sessions should be carefully considered and purpose-driven. Most boards opt to exclude the company secretary unless their presence is essential and agreed upon in advance such that open discussion among directors is not impeded and to avoid the company secretary being placed in an awkward position, especially if they are privy to sensitive discussions which cannot be disclosed to management. Rather, the chair can communicate any resolutions or decisions that need to be formally recorded to the Company Secretary afterwards and the chair can document confidential minutes (if required) and store these separately for director only access.

BOARDROOM CONDUCT

Boardroom conduct and behaviour has a significant impact on board effectiveness, yet it is one of the most difficult things for boards to deal with. Negative behaviours such as lack of engagement, aggression, dominance, bullying and exclusiveness entering the boardroom can distract directors from their responsibilities, creating rifts, factions or divisions that can take considerable time and effort to resolve. In particular, the non-essential use of mobile phones should be discouraged during board meetings.

It is in the best interests of individuals – and the organisation – for boards to engage in collegiate, constructive and respectful behaviours.

While each board will have its own boardroom style, there are basic principles of good boardroom practice and etiquette:

- punctuality and attendance for the full meeting
- full attention should be given to listening and contributing to the discussion
- well-timed and adequate breaks should be scheduled, and catering provided, especially for long meetings.

The chair's role is critical in managing the conduct of meetings, with directors needing to take accountability for their behaviour, ensuring that it meets the expected norms and behaviours for a safe, constructive working environment for everyone involved.

Beyond this, a board may have best practice processes and administration yet still struggle to make decisions or effectively monitor the performance and risks of the business, due to problematic dynamics and habits.

A recent Harvard Law School Forum on Corporate Governance article¹⁰ highlights key threats to effective board performance include a tendency for risk aversion or paralysis in the face of multiple issues, including maintaining a commitment to an initiative (to justify an investment and avoid cutting losses) rather than admitting that a strategy may not be achieving the desired results. The study also highlighted the importance of emotional intelligence and psychological safety. Recognising that everyone contributes a range of diverse and deep experience, there is growing recognition 'that the boardroom with the smartest people doesn't guarantee a better functioning board or better oversight'. The importance of social sensitivity and cohesion, built on equitable, face-to-face contributions and a good level of emotional intelligence, can create a richer and more trusted dialogue.

CONFIDENTIALITY

Consistent with their fiduciary duties, directors are expected to maintain the confidentiality of the deliberations of the board and its committees. Confidential company papers must remain secure. It is recognised as best practice for directors to return meeting papers to the company secretary after the meeting, who will then arrange for the secure destruction of surplus copies.

Several fundamental security recommendations include:

- encrypting documents
- installing password protection mechanisms for all electronic equipment
- activating automatic locking after periods of inactivity on electronic devices
- careful use of PINs for conference calls.

¹⁰ Harvard Law School Forum on Corporate Governance, Why good boards make bad decisions, 11 February 2024, <https://corpgov.law.harvard.edu/2024/02/11/why-good-boards-make-bad-decisions/>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

INDEPENDENT PROFESSIONAL ADVICE

When one or a number of directors have concerns about the advice given to the board in relation to an issue, the board may need to seek independent professional advice to properly discharge its responsibilities.¹¹ The board should have authority to obtain advice, reports or opinions from expert advisers, as deemed necessary, at the expense of the company. Controls should be in place to ensure the process is properly managed.

BOARD MINUTES

The Corporations Act provides that a company must keep a record of the proceedings and resolutions of directors' meetings, including meetings of a committee of directors, and any decisions taken outside the meeting, such as those passed by a rotary/circulating resolution.¹²

The company secretary is responsible for preparing the minutes from notes taken at the meeting, and should provide a draft copy to the chair within an agreed reasonable time frame. KPMG recommends that this should not exceed five days such that draft minutes can be circulated to other directors for information as soon as possible after the meeting (KPMG suggests that good practice is to do this within 14 days). The minutes must be posted in the minute book (which can be digital) within one month of the meeting and signed within a reasonable time by the chair of the meeting or the chair of the next meeting.¹³

Minutes should be compiled very carefully and with appropriate detail, with due regard to the fact that minutes provide evidence of what has occurred in meetings and can be used as documents with legal significance in instances of litigation. With an increasing responsibility on directors to be able to show they have properly undertaken their duties, proper minutes can protect directors in this respect.

It is therefore essential that directors give the process of reviewing and approving the minutes the level of attention it warrants, rather than simply treating it as an administrative exercise. Once signed, minutes are evidence of a proceeding, resolution or declaration to which it relates (unless the contrary is proven).¹⁴ Criminal penalties can be imposed for the falsification of records.¹⁵ Minutes may be used in court to prove or disprove that directors have fulfilled their duties (as was evidenced in the James Hardie case).

If errors are subsequently detected in signed minutes, directors may pass a resolution at a future meeting to correct them. The directors may agree not to proceed with an agreed course of action as set out in the signed minutes. In these circumstances, it will be necessary for the directors to pass a resolution to rescind previous resolutions.

The minutes should always be formally approved at the next meeting if they have not previously been formally approved by all the members of the board. If the minutes are amended at the next board meeting, this should be reflected in the minutes of the subsequent meeting.

The company is responsible for safely and indefinitely keeping the minute books at the company's registered office, principal place of business or another place approved by ASIC.¹⁶ Minutes can be stored in a bound or loose-leaf format or electronically, as long as they can be reproduced in a printed form.¹⁷

11 ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Commentary to Recommendation 1.1.

12 Corporations Act 2001, Sections 251A(1)(b) and 251A(1)(d).

13 Corporations Act 2001, Sections 251A(1)(b) and 251A(1)(d).

14 Corporations Act 2001, Section 251A(6).

15 Corporations Act 2001, Section 1307.

16 Corporations Act 2001, Section 251A(5).

17 Corporations Act 2001, Section 1306.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The level of detail included in the minutes will vary from company to company. General inclusions would be:

- company name
- meeting location, date and commencement time
- chair and attendee names, including those physically present and those participating through the use of technology (e.g. teleconference)
- apologies
- presence of a quorum
- minutes of the previous meeting
- directors' declarations of personal interest
- proceedings and resolutions (including a brief outline of material factors in reaching a decision)
- title, version reference and date of all papers tabled
- directors' disclaimers or objections
- action plans, timelines and responsibilities for implementation
- closure time
- signature of the chairman (at the subsequent meeting).

The original minutes with the amendments noted should be retained to demonstrate compliance with section 251A of the Corporations Act, and to avoid any suggestion of destruction of company records in contravention of section 1306 of the Corporations Act.

TECHNOLOGY

A directors meeting can be called or held using any technology, provided that all directors consent.¹⁸

This is obviously useful when a director cannot physically participate in a meeting. Emergency meetings called at short notice are a case in point. Whilst the use of meeting technology for virtual meetings can eliminate many hours of travel time for directors located interstate or overseas, face-to-face meetings are often preferred, especially where contentious matters are to be discussed. It is fundamental where technology is used, that it is secure (particularly given the commercially sensitive nature of discussions), reliable and fully functional.

KPMG recommends that at least two meetings a year be conducted face to face, in addition to any strategy dedicated sessions such that the directors can form a connection and build a level of trust that is sometimes more difficult to achieve in a virtual meeting.

With the advent of AI and transcript recording tools, the temptation to record meetings and have minutes generated through these tools is a temptation. However, the same policies should apply to recording meetings as existed before virtual meetings became commonplace. Typically, recording board (or committee) meetings is not recommended because it is likely to reduce free-flowing discussion among directors which will affect necessary candid debate and deliberation. In addition, having meetings recorded introduces legal and evidentiary risks, especially in litigation or regulatory investigations.

¹⁸ Corporations Act 2001, Section 248D.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

If it is decided that recordings are to be made (e.g., for minute drafting purposes), the Governance Institute of Australia (GIA) recommends:

- Destruction after the minutes are approved; and
- Disclosing of the practice for the board to agree upon.¹⁹

The AICD emphasizes that minutes are a record of decisions and proceedings, not a transcript or detailed report of individual contributions or debate. Overly detailed minutes can be as problematic as insufficient ones.²⁰

A joint statement by GIA and AICD reinforces that AI tools may assist in drafting minutes, but human oversight is essential to ensure accuracy and integrity.²¹

MEETING EVALUATION

The meeting should conclude with a review of decisions reached and the related actions, in order to increase accountability among directors. All participants should be fully aware of what is expected of them. Following the meeting, the company secretary should ensure the minutes are circulated quickly in order to allow directors to promptly respond.

Requesting feedback on the meeting will provide valuable insights into how future meetings may be made more productive.

Useful resources

- Australian Institute of Company Directors and Governance Institute of Australia, *Joint statement on board minutes (2019)*, <https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/board/board-minutes-director-tools.pdf>
- Australian Institute of Company Directors and Governance Institute of Australia, *Joint Statement on board minutes and the use of AI* <https://www.governanceinstitute.com.au/advocacy/thought-leadership/joint-statement-on-board-minutes/>

For further information please contact:



Caron Sugars

**Lead Partner,
Board Advisory Services
KPMG Australia
ccobargsugar@kpmg.com.au**

¹⁹ Governance Institute of Australia, Good Governance Guide – Management and oversight Issues to consider when recording and circulating minutes of directors' meetings, November 2023, https://www.governanceinstitute.com.au/app/uploads/2023/11/ggg_issues_consider_recording_circulating_minutes_directors_meetings.pdf

²⁰ AICD, New guidance for directors on minute-taking law and practice, 15 August 2019, <https://www.aicd.com.au/board-of-directors/meeting/minutes/new-guidance-for-directors-on-minute-taking-law-and-practice.html>

²¹ Governance Institute of Australia and AICD, Effective Board Minutes and the Use of AI A Joint Statement. May 2025, <https://www.governanceinstitute.com.au/app/uploads/2025/05/Effective-Board-Minutes-and-the-Use-of-AI.pdf>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

14. Strategy and Planning

Boards are responsible for ensuring the company is sufficiently agile to respond to changes in the business and economic environment and be able to capture emerging opportunities.

In this chapter

- Corporate strategy
- Defining the board's role in strategy
- Defining the chair's role in strategy
- Defining the committee's role in strategy
- Understanding shareholder value
- Sustainable competitive advantage
- Thinking strategically
- Stakeholder involvement in strategic planning
- Strategic risk
- Strategy review
- Using the 'balance scorecard'

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. At the start of the strategy development process, does the board provide management with directional guidelines?
2. Has the board and management defined shareholder value and how it is measured?
3. Does management ensure that all strategic initiatives presented to the board are designed to enhance shareholder value, but with appropriate consideration of other relevant stakeholders?
4. Do the board and senior management hold an annual strategic planning day(s) to discuss and approve strategic objectives?
5. Does the board challenge and question management to achieve better strategy formulation based on mutual respect, open and honest communication and candid debate?
6. Is understanding of strategic and emerging risk incorporated into strategic planning?
7. Does the board incorporate risk management into its strategic decision-making process?
8. Does the strategy include scenario analysis such that the strategy can easily pivot when scenarios change?
9. Does the board drive management to develop a business model that provides the organisation with a competitive advantage?
10. Are the strategic options presented by management based on robust and thorough analysis using established tools and methodologies?
11. Does management have an environment scanning process to capture new technologies, consumer trends, competitor tactics and other significant external changes?
12. Are the views of key stakeholders taken into account in the strategy development process?
13. Are different strategic options considered prior to a final decision being made by the board?
14. Does the board ensure that there is a rigorous process in place to translate the strategy into action through corporate budgeting and planning?
15. Have board and management considered using the 'balanced scorecard' approach to measure the organisation's performance?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The board accepts management's strategy without in-depth probing or questioning.
- The board does not fully understand the nature and implications of the proposed strategy.
- The external environment is not fully considered in strategy development.
- Not all directors attend the meeting when the strategy is discussed and approved.
- The risks inherent in strategy are not identified or managed.
- Strategic decisions are not adhered to or are revisited excessively.
- The mechanisms for measuring shareholder value are not fully understood.
- Board meetings are not strategically focused.
- There is little time devoted to non-financial performance measures.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

CORPORATE STRATEGY

The performance dimension of a board's role focuses on business strategy and the pursuit of shareholder value.

The nature and extent of the board's participation in strategy depends on the company's size, industry and particular circumstances. It is, however, essential that cooperative and interactive strategic planning processes are instituted which enable boards and management to:

- make, review and assess strategic decisions
- understand the key drivers of company performance
- align the company's strategy, operations and external environment
- understand potential risks and incorporate risk management into strategic decision-making.

DEFINING THE BOARD'S ROLE IN STRATEGY

The long-held view that the board's role is limited to reviewing, understanding, and signing off on the strategy has given way to deeper board engagement on a company's strategy. Increasingly complex business conditions demand it, investors and stakeholders expect it, and ASIC and other professional bodies have urged boards to be more strategic, focusing on future performance, as well as compliance. Many directors believe strategy to be their most important sphere of activity, with their input having a significant influence on company performance.

Directors can have a meaningful impact on the strategy process. Factors to assist in enabling this include:

- strong knowledge of the company's operating context, and external environment
- allocating sufficient time to consideration of strategic issues
- board time not being overly taken up with compliance issues
- executives being willing to incorporate director input

- having a dedicated forum for participation (such as a specific strategic planning workshop)
- management discussing options with directors rather than presenting a 'final' strategy.

However, the foundational element is the board providing clarity on what the risk appetite of the organisation is. Without this, it is very difficult to assess whether a strategy is too bold, too timid or has hit the right balance.

Reviewing, adding value to and approving the strategy are crucial to the board's governance role, and KPMG's experience in talking to boards and undertaking board performance assessments is that directors almost always would like more time on strategy. Unfortunately, with an increased focus on compliance, strategy has been allocated less time on the board agenda – notwithstanding that this is often the area in which directors feel that they add the most value.

Boards need to be seen by management as a strategic resource that contributes to superior company performance. Through the board's unique position, directors can contribute by providing:

- market information and industry trends
- experience and expertise accumulated during their professional careers
- new perspectives and fresh ideas
- an independent and objective viewpoint.

These strengths, combined with management's in-depth company knowledge and experience, mean that collaborative decision-making often leads to better strategy. Directors are more likely to add value to the strategy process if they possess a strong understanding of the company and its environment, have strong meaningful working relationships with each other, as well as the management team, and are able to communicate and exchange information.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

DEFINING THE CHAIR'S ROLE IN STRATEGY

Chairs KPMG speak to consistently emphasise three key areas of focus for chairs as they facilitate their board's engagement in the strategy process, from strategy development and evaluation to monitoring strategic execution and recalibrating strategy as necessary:

- **Setting expectations** with the CEO and directors for the board's engagement in strategy.
- **Planning the set-up** and staging of board strategy discussions and providing the backdrop to drive the right focus and dynamics.
- **Building consensus** about the proposed direction of the strategy – the forty-thousand-foot view

Chairs also emphasised a number of specific elements and practices that are pivotal to quality boardroom discussions about strategy, e.g. diverse and dissenting views, having a vivid picture of the future, and focusing on critical alignments:

- Encourage the board, CEO, and management to develop a vivid picture of the future, where the industry and competition are headed and its impact on strategy.
- Insist on diverse and dissenting points of view, including third-party input.
- Assess whether the company's strategy process enables the company to recalibrate strategy as needed while maintaining critical alignments.
- Work with committee chairs to maintain the alignment of board and committee structure and governance processes with strategy.
- As part of the board evaluation, assess whether the board has the right composition and leadership to effectively engage in strategy.

DEFINING COMMITTEES' ROLE IN STRATEGY

As boardroom leaders, committees can offer a unique perspective on strategy. At least annually, consider the company's strategy through the committee lens; revisit committee responsibilities, work plans, and evaluations to help ensure alignment with the company's strategy and its drivers.

- **Nomination committees** should be focused squarely on board composition and talent. Do we have the talent around the boardroom table to effectively evaluate the strategy? Is the board fit for purpose and able to help guide the company into the future? More broadly, consider with the remuneration committee whether the company has the right talent to implement the strategy.
- **Remuneration committees** should ensure that remuneration plans are synchronised with strategy, particularly as strategies change in light of industry transformation and disruption. Old metrics and incentives may no longer relate to the new strategy. Is the organisation attracting and retaining the talent required to execute its strategy?
- **Audit committees** may need to sharpen their focus on capital investments and capital allocation as well as the overall culture and control environment, particularly as the strategy changes.
- **Other committees** – Is a new committee needed? As the operating environment gets more complex, an additional committee (e.g. to oversee technology, risk, or public policy) might make sense. However, this needs to be considered in light of whether the board has the bandwidth and necessary skillsets for an additional committee.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

UNDERSTANDING SHAREHOLDER VALUE

The board and management must ensure all strategic initiatives are designed to enhance shareholder value, balanced with appropriate consideration given to other relevant stakeholders and overall ESG objectives. Shareholders define value from a different perspective to the company. To shareholders, value may be simply the dividends or cash equivalents they receive, plus the increase (or decrease) in the market value of their shareholdings over the life of their investment. Companies require more objective measures of shareholder value that are independent of the volatility and ambiguity of market valuations. It is important for boards to define and measure shareholder value. This definition will guide decision-making at all levels of the organisation.

SUSTAINABLE COMPETITIVE ADVANTAGE

The fundamental aim of corporate strategy is to provide an organisation with sustainable competitive advantage. This refers to the unique value-creation that sets an organisation apart from its competitors. Sources of competitive advantage may include:

- a compelling customer experience or proposition
- dynamic product lines
- use of a leading-edge business model
- innovation
- effective use and sharing of assets and resources, such as patents and other intellectual property, corporate reputation and physical locations
- the collective skills and experience of the executive and management team
- strong and clear focus.

Most competitive advantages are short-lived because environments change rapidly. Creating sustainable competitive advantage over the long term necessitates that companies be flexible and responsive. In fact, organisational agility and the ability to redeploy organisational resources to take advantage of opportunities can be a sustainable competitive advantage in itself.

THINKING STRATEGICALLY

Thinking strategically is distinct from strategic planning. Whereas strategic planning is often a formal process, driven by analysis and consideration of different strategic options, strategic thinking is a more continual, creative process whereby individuals approach problems from a broader perspective. Boards are removed from the everyday running of the company, and are therefore in an ideal position to employ strategic thinking.

Boards should develop a culture of strategic thinking that can be assisted by:

- creating a climate where strategic thinking is a valued activity
- challenging and evaluating the processes for developing strategy, not just the strategies themselves
- upholding high expectations for strategic plans
- setting aside adequate time and resources to discuss strategy in a meaningful way
- establishing methodologies, tools and policies for strategic decision-making and monitoring management adherence to them
- ensuring company decisions align with the strategy and the inter-related risk appetite.

STAKEHOLDER INVOLVEMENT IN STRATEGIC PLANNING

A critical step in the strategic planning process is engaging with key stakeholders. A company's stakeholders are those groups who affect and/or are affected by the company and its activities, such as investors, lenders, analysts, employees and customers. In leading organisations, stakeholder engagement has migrated from an optional consideration to an integral part of the business strategy.

Boards face ongoing scrutiny and increasingly high expectations from stakeholders. As part of their responsibility for governance oversight, directors need to identify and understand the expectations of the company's stakeholders, which may vary across industries and are continually changing.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The ASX Principles suggest that to make ethical and responsible decisions, companies should not only comply with legal obligations, but should also consider the reasonable expectations of their stakeholders.¹ It is considered good practice to incorporate stakeholder views into the strategy development process, whether directly through consultation with stakeholder representatives, or by indirectly acknowledging their goals when generating strategy. Stakeholders bring expert advice or represent the interests of groups that can have a major effect on the success of the strategy. A diverse range of views and ideas can lead to more innovative problem-solving. There should also be enhanced communication and trust, leading to mutual understanding and collaboration, and reduced legal and reputational risks and associated costs.

STRATEGIC RISK

Boards must identify, assess and manage the risks inherent in any strategic plan. Strategic plans often do not achieve their desired aims, are poorly executed, or fail to keep pace with changes to the business environment.

Directors have a duty to satisfy themselves that an effective strategic risk management plan is in place and is being followed. Such plans should:

- identify and evaluate strategic risks
- consider non-financial in addition to financial risks
- consider emerging risks and trends
- reflect the organisation's risk appetite
- measure what is happening
- be aligned with the organisation's delegation of authorities
- prepare for, and take appropriate corrective action.

Boards must try to balance both short- and longer-term strategic risk. Strategic risk increases as the time horizon expands – the longer the time frame, the more unpredictable it becomes, and thus the more sophisticated the organisation's risk management capabilities need to be. Many organisations develop scenarios that deal with a variety of alternatives to mitigate this problem. Risk management is an increasingly vital part of organisational accountability and strategic decision-making. Accordingly risk and strategy feed each other as emerging and existing risk informs strategic direction and then the strategy informs what strategic risks will need to be managed.

STRATEGY REVIEW

Strategy needs to be continually reviewed. It is the board's responsibility to conduct a thorough analysis of current strategy and progress towards the agreed objectives, and to evaluate company performance in light of these objectives. A board will normally review the strategic direction at least annually, with an increasing trend to half-yearly reviews. Strategies should also be subject to reviews to ensure they remain appropriate to the organisation's needs. There is a danger that organisations become complacent in their strategy, making incremental adjustments while their environments continue to change rapidly. More agile competitors can overtake companies that merely react to the environment, rather than challenging, questioning, and even influencing it.

In addition, boards need to be vigilant in assessing company performance in achieving the strategy. Periodic reporting from management (such as a quarterly report card incorporating exception reporting) can help the board quickly come to terms with what is not working and why. Boards need to ensure that sufficient funds and resources are provided to enable an organisation to achieve its strategic goals.

¹ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Principle 3.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

It is important that the board receives the appropriate facts and information to make an accurate assessment. Financial and operational reports are a good starting point, but the board also requires non-financial performance indicators. These may include indicators of customer satisfaction, employee engagement; health, safety and wellbeing; and community involvement. The board is there to look objectively at company strategy and make the difficult decision to change a company's course when it is no longer viable.

Rather than trying to predict the future, the board can ensure the organisation's capabilities and resources are sufficient to manage uncertainty and that strategic plans are flexible. In-built flexibility is promoted by:

- scanning the environment constantly and keeping abreast of changes that could materially affect the achievement of strategic objectives
- exploring how environmental shifts will impact on strategy
- inviting subject matter experts to address the board and senior management
- ensuring accurate and timely information reaches the board and is discussed candidly by directors and managers by scheduling breakout sessions to allow the board to critique the current strategy.

USING THE BALANCED SCORECARD

The balanced scorecard method is used by many companies globally as a better practice approach to setting performance measures and subsequently measuring actual performance. The idea of a balanced scorecard arises from the fact that financial measures are the end result of a range of other activities and processes taking place in companies. To increase sales, cut costs, lift margins, raise profits and improve return on investment, companies must do things such as engage in activities, processes, programs and projects. Directors must get behind the financials to discover these value drivers. They must learn to measure the value drivers if they are to manage them.

The balanced scorecard approach recommends that boards view their business from many perspectives.



Financial perspective – How does our performance look to shareholders? Are we adding value?



Customer perspective – How do customers see us?



Internal business perspective – What must we excel at?



Innovation and learning perspective – Can we continue to innovate and create value?



Community and environment – How do we meet all key stakeholder expectations?

Using a balanced scorecard approach, companies set themselves goals or business objectives for each perspective. They then select the measures that best track progress in achieving these goals. These goals and measures should be geared to the circumstances of individual companies.

The balanced scorecard provides a performance information framework that allows companies to evaluate the effectiveness of their strategy. The balanced scorecard methodology has been promoted mainly as a management process, but it makes an excellent reporting framework for company boards.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- AICD (Tools & Resources> Director tools> Board, Strategy)
<https://www.aicd.com.au/tools-and-resources/director-tools/board.html>
- KPMG, 2019, Facilitating the board's engagement in strategy,
<https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2019/12/facilitating-the-boards-engagement-in-strategy.pdf>

For further information please contact:



Ryan Wolton

**National Leader, KPMG Strategy
KPMG Australia
rwolton@kpmg.com.au**

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

15. Receiving Assurance

Whilst the board may understand its business risks well, without comprehensive assurance, the board has no way of knowing that the business is managing these risks appropriately.

In this chapter

- The role of assurance
- The role of the audit committee
- Internal risk and compliance frameworks
- Internal audit
- External audit
- Assurance over sustainability reporting
- Analytics and assurance
- Artificial intelligence (AI) in assurance
- Other assurance providers

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Is the board/audit committee satisfied with management's assurances in relation to the company's risk management and internal control and compliance systems?
2. Does the board receive regular independent assurance on the effectiveness of the business risk management framework and controls?
3. Has an assurance map been developed that provides a consolidated view on how assurance across the organisation's key processes and/or risks is obtained?
4. Does the external auditor test and challenge elements of the financial reporting, disclosure, risk and control environment?
5. Does the board receive assurance over other non-financial disclosures made by the company (e.g. environmental, social and governance (ESG) related disclosures)?
6. Is the board, through the audit committee, satisfied that the internal audit function is operating effectively and efficiently?
7. Is the internal audit plan clearly linked to the most current risk profile, and is the risk profile updated based on audit findings and outcomes?
8. Are remedial actions resulting from weaknesses identified by assurance activities monitored by the audit committee?
9. What is the status of open actions resulting from assurance activities, and are overdue items escalated appropriately?
10. Is management invited to the audit committee to discuss key assurance outcomes (e.g. high or critical rated assurance findings) with the board?
11. Does the audit committee have a defined escalation process in place for any critical risks identified in assurance activities?
12. Do the board and relevant committees have the right skills and experience to provide oversight and challenge to the internal and external auditors?
13. Do both the external and internal auditors meet with the chair of the audit committee without management attending, as well as have the opportunity to present at each audit committee meeting?
14. Are there board approved charters in place for the roles and accountabilities of the external and internal auditors?
15. Is the assurance planning aligned with risk management and strategic planning?
16. What insights can assurance provide about the organisation?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- Assurance is limited to financial processes only.
- The board does not review the risk profile and internal audit plan on a periodic basis.
- The assurance findings do not align with the perceived control framework effectiveness on which the overall risk profile is based.
- Uncertainty exists over the processes supporting management attestations.
- The internal audit function appears to be under-resourced or projects are being cancelled or delayed by management.
- Recommendations made by assurance providers are not being tracked and implemented.
- An assurance map does not exist to indicate any gaps in assurance provided.
- The audit committee reports to the board do not provide an overview of the internal audit work plan and outcomes.
- The board becomes aware of significant accounting disagreements between management and the external auditors.
- The external auditors are not present when the board considers the annual financial statements.
- Accountability and responsibility at management levels for issues identified through assurance processes and the associated resolution is shared across multiple roles, or unclear.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

THE ROLE OF ASSURANCE

Assurance can be described as an assessment process from which a level of confidence over the matter under review can be gained. Boards should obtain comprehensive assurance on the effectiveness of their organisation's business risk management and compliance frameworks, and the controls applied to manage these.

Assurance can be sought by the board for dual purposes, as a means of gaining comfort over the implementation and effective management of **internal** controls over organisational risks, and, to provide **external** stakeholders with an independent assessment of how well an organisation is meeting mandatory or voluntary performance and reporting standards.

Assurance can take a number of forms including:

- system-based reporting produced from the implementation of risk and compliance frameworks
- management attestations and assurances
- internal audit
- external audit
- other independent assurance providers (e.g. actuarial, WH&S, independent experts).

THE ROLE OF THE AUDIT COMMITTEE

Listing Rule 12.7 requires ASX listed companies included in the S&P/ASX 300 index to have an audit committee. Recommendation 4.1 of the ASX Principles also suggests that a listed entity have an audit committee. The commentary to Recommendation 4.1 lists those matters which the audit committee should make recommendations to the board regarding.

The audit committee's key duties and functions relating to internal audit include:

- reviewing the internal audit charter to ensure the appropriate organisational structures, authority, access and reporting arrangements are in place
- assisting the board to ensure senior management establishes and maintains adequate and effective internal controls
- overseeing the scope and effectiveness of the assurance systems established by management to identify, assess, manage and monitor the various business risks arising from the organisation's activities
- reviewing the scope and coverage of the internal audit plan, annual work plan, and monitoring progress
- advising the board on the adequacy of internal audit resources to carry out its responsibilities, including completion of the approved internal audit plan
- reviewing internal audit reports and advising the board on significant issues identified and the actions taken (including the identification and dissemination of good practice)
- monitoring management's implementation of internal audit recommendations
- assisting the board to oversee that appropriate controls are in place for the monitoring of compliance with laws, regulations, supervisory requirements and relevant internal policies
- periodically assessing the performance and objectivity of the internal audit function
- making recommendations for the appointment (or if necessary, the removal) of the head of internal audit.

The audit committee should be involved in setting the internal audit's functions and goals. These should be incorporated into the internal audit charter or in an appropriate service level agreement. The internal audit charter defines the audit committee's expectations for the internal audit function.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Typically, the audit committee should expect the following components to be included in the internal audit charter:

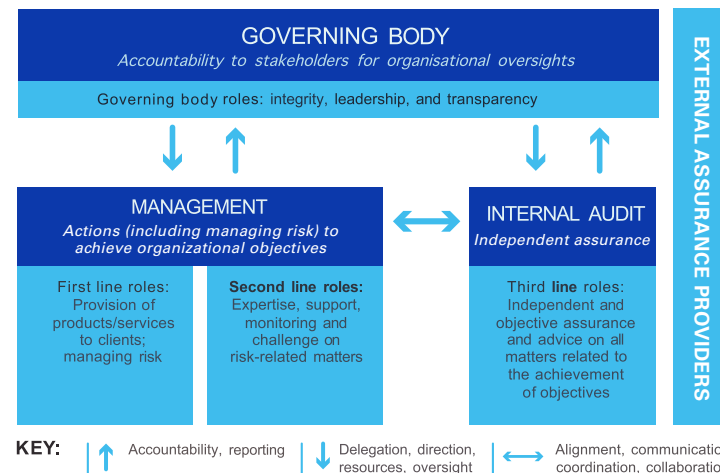
- role and scope of work
- responsibility and accountability
- objectivity and independence
- operating principles
- reporting, including an overview of reports to be completed throughout the year
- quality of service, including management feedback.

It is common practice to combine the audit and risk committees which serves to even further align the assurance activities with the risk management functions.

INTERNAL RISK AND COMPLIANCE FRAMEWORKS

Most organisations establish a control environment that is commonly referred to as the 'three lines model' or 'three lines governance model' (previously, 'three lines of defence'). The Institute of Internal Auditors' illustration of this model is included below.

The IIA's Three Lines Model



Source: The IIA's Three Lines Model – An update of the Three Lines of Defence

The three lines works on the basis of establishing controls within different layers of the organisation, starting at the operational level as the first line, where controls are in place to manage day-to-day risks (e.g. the bank teller validating a customer's identity when they withdraw cash to help mitigate fraud risk). The second line relies on oversight functions within the business, which establish and oversee systemised governance approaches that support the first line. For example, the finance team of the bank checking transactions to ensure that the correct identification from the customer was sought during the withdrawal and that a reconciliation of funds withdrawn for the day is regularly performed to identify any potential errors. The third line is independent assurance over these processes, where reviewing and testing by an independent party is performed and reported to the board (potentially through an audit committee or similar), identifying any errors or control weaknesses.

Boards should obtain a level of assurance or comfort on the soundness of the systems of management controls over key risks from risk management reporting. The degree of assurance will depend upon the robustness of the risk management process. Boards should understand this process well and ensure that it is regularly reviewed and updated. At least in theory, receiving attestations from management allows the board to regularly satisfy itself about the veracity of the company's outputs, processes, systems and controls.

The scope of these attestations can include:

- the integrity of the financial reports
- effective risk management, internal compliance and management control systems over financial reporting risks and material business risks
- compliance with company policies and regulatory requirements.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The Corporations Act and ASX Principles formalise the management sign-offs relating to the financial reports. Section 295A of the Corporations Act requires the CEO and CFO of a listed company to provide the board with an annual written declaration and sign-off that the company's financial records have been properly maintained, the annual financial statements comply with accounting standards and give a true and fair view of the company's financial position and performance.

Further, the ASX Principles recommend that the declarations required under section 295A extend to include a declaration from the CEO and CFO that the financial statements have been formed on the basis of a sound risk management system and internal controls which are operating effectively. It also extends the need for the declaration to apply to the financial statements for any financial period, not just the financial year end.¹

The ASX Principles also recommend that a listed entity should disclose:

- if it has an internal audit function, how the function is structured and what role it has, or
- if it does not have an internal audit function, that fact and the processes it employs for evaluating and continually improving the effectiveness of its risk management and internal control processes.²

An internal audit function can assist a listed entity to accomplish its objectives by bringing a systematic, disciplined approach to evaluating and continually improving the effectiveness of its risk management and internal control processes.³

INTERNAL AUDIT

An effective internal audit function plays a key role in helping the board, through the audit committee, to discharge its governance responsibilities. As such, the audit committee needs to satisfy itself that internal audit is functioning effectively and efficiently.

- 1 ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, commentary to Recommendation 4.2
- 2 ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, commentary to Recommendation 7.3
- 3 ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, commentary to Recommendation 7.3

A strong relationship between the audit committee and the entity's internal auditors enables the committee to meet its responsibilities and carry out its functions. Internal audit should be a major source of information to the audit committee on the performance of the entity.

Australia's position in the global market, changes to corporate governance requirements and the dramatic changes in the business operating environment have increasingly brought about a need for the board, through its audit committee, to seek broader assurances beyond financial matters in a range of areas, including: core operations; major projects and/or transformation initiatives; health, safety and wellbeing; environment; security; information systems; and human resources to name a few. These quality assurance needs have broadened the traditional internal audit function. The new-style internal audit model is aligned directly with corporate strategy and focuses on specific risks that influence organisational success.

Internal audit has a multifaceted role to play in the enterprise risk management (ERM) arena. The Institute of Internal Auditors in Australia notes that internal audit's core role with regard to ERM is to provide objective assurance to the board on the effectiveness of an organisation's ERM activities to help ensure key business risks are being managed appropriately and that the system of internal control is operating effectively. In addition, many companies are looking to internal audit to support strategic business objectives. That effort extends to ERM activities such as:

- risk identification and prioritisation
- alignment of people, processes and systems with the business strategy
- definition of key performance indicators
- analysis and quantification of risk factors in new business ventures and strategies
- understanding the shared risks among various projects and initiatives
- evaluating and supporting the improvement of organisational risk culture.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Internal audit's role, its knowledge of the organisation's key risks, and its enterprise-wide view enable it to bring an important perspective and discipline to an ERM effort.

Forward-thinking organisations are those that do not view compliance risk management as a cost of doing business, but rather as a strategic investment that is critical to business resilience, efficiency and success. This trend towards strategic compliance risk management requires a bespoke approach to the design and development of compliance arrangements. A one-size-fits-all approach to the design of compliance arrangements is not always appropriate or practical.

Risk-based internal audit plan

In reviewing the internal audit plan, audit committees need to consider the risk profile and determine the areas where internal audit can provide assurance. In making this judgement, directors need to be aware that, where the internal audit function is in-house, there may be some issues that will require coverage by additional specialists through an independent third-party review. The audit committee should ensure the internal audit team has used a formal process to define and prioritise risks and plan its work accordingly. A risk-based internal audit plan can prioritise the key risks subject to audit and allocate focus over the internal audit cycle. The plan should also be flexible so that emerging risk issues can be incorporated into the program.

Scope, procedures, coverage and timing

The proposed scope, procedures, coverage and depth of the internal audit plan, and particularly any restrictions on the scope of the internal audit plan, should be fully discussed and debated by the audit committee before being approved. The audit committee should ensure that strategic business risks have been evaluated and assessed with respect to determining the audit procedures and scope. The audit committee should consider the timing of proposed audit work and prioritise, where necessary.

Internal audit results

Regular communication by the internal audit function with the audit committee is critical, especially with regard to the completion of reported findings and recommended improvements. A timetable for regular meetings and proposed internal audit report completion dates should be included in the internal audit plan. The audit committee should have mechanisms for facilitating confidential exchanges with the internal auditor. This can be by way of the audit committee chair meeting with the head of the internal audit function outside audit committee meetings, or meetings (adjunct to the formal committee meeting) between the audit committee and the internal auditor 'in camera' (without management present).

The reporting to the audit committee should not cease when the internal audit report on findings is tabled. Rather, the internal auditor should report to each meeting on whether actions agreed to be taken to remediate the weaknesses noted have been completed to an acceptable level by the due dates. This enables the audit committee to understand whether the risks identified have been mitigated, or whether further resources need to be applied to achieve resolution. Internal audit functions may elect to leverage governance, risk, compliance (GRC) technological tools (software) to facilitate the capturing, monitoring and reporting of findings and agreed management actions.

Operational changes and new developments

Audit committees and the internal audit function need to keep abreast of developments affecting its activities and internal audit work. The internal audit function should be responsive to changing needs, striving for continuous improvement and monitoring integrity in the performance of its activities.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Budget, staffing and resources

The audit committee should ensure the internal audit function is appropriately staffed and resourced. To allow for full accountability, the budget should include a detailed analysis of time and/or cost per project. If a third-party provider acts as the internal auditor, an engagement letter should also be signed to formally set out the mechanism for developing and agreeing a plan and budget.

So as to enable internal audit to extend into all aspects of the business, as well as to create opportunities for talented staff to understand assurance and risk management, some progressive organisations utilise 'guest auditors' from within the operations to join the internal audit team and provide subject matter expertise into the topic being audited.

EXTERNAL AUDIT

The external auditor, as an independent party with knowledge of the entity's financial affairs, is in a position to provide the board (through the audit committee) with independent insight into the effectiveness of the organisation's risk management, internal control, financial reporting and legislative compliance frameworks. As such, the external auditor can be an important contributor to good governance.

One of the key functions performed by the external auditor is the audit of the company's annual financial report. The auditor must report to members on whether, in the auditor's opinion, the financial report complies with the Corporations Act, accounting standards and gives a true and fair view of the financial position and performance of the company.⁴ The auditor must also provide the directors with an independence declaration, i.e. a declaration that, to the auditor's knowledge and belief, that there have been no contraventions of the auditor independence requirements under the Corporations Act or any applicable professional code of conduct in relation to the audit.⁵

4 See Part 2M.3 Division 3 of the Corporations Act generally as to the audit and auditor's report. See also [Chapter 7](#) (Accountability to shareholders).
5 CA 307C.

Other functions carried out by an external auditor will also generally include evaluating elements of the control environment covering financial reporting and providing suggestions to improve the effectiveness of financial control, management and reporting and disclosure.

The audit committee typically has significant engagement with the external auditor throughout the year. Some of the key functions performed by the audit committee in assisting the board in its oversight of the external auditor include:

- developing and implementing procedures for the selection, appointment and rotation of the external auditor
- recommending to the board the appointment or (if necessary) the removal of the external auditor
- reviewing and (if appropriately authorised under the delegations framework) approving the terms of engagement and the reasonableness of the audit fees prior to the commencement of the audit
- reviewing and (if appropriately authorised under the delegations framework) approving the external auditor's proposed audit plan and audit approach, including materiality thresholds
- assessing the performance and objectivity of the external auditor.⁶

The Auditing and Assurance Standards Board (AUASB) is an independent statutory agency of the Australian Government which is responsible for developing, issuing and maintaining auditing and assurance standards. The AUASB Standards establish requirements and provide explanatory material on the responsibilities of the auditor and the assurance practitioner, as appropriate, when performing audits, reviews, assurance or related services engagements.⁷ Directors on an audit committee should have a general understanding of the standards and how these apply to the external auditor in the external audit process.

6 ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, commentary to Recommendation 4.1.

7 Refer to Auditing and Assurance Standards Board, <http://www.auasb.gov.au/Home.aspx>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Section 250RA of the Corporations Act requires an auditor of a listed entity to attend the entity's AGM and be available to answer questions from shareholders relevant to the audit.⁸ For those listed entities established outside of Australia, Recommendation 9.3 recommends that the entity should ensure that its external auditor attends its AGM and is available to answer questions from security holders relevant to the audit.

Communication with the external auditor

It is important that the audit committee communicates to the external auditor any matters relevant to the planning and completion of the audit. At the start of each annual external audit cycle, the audit committee needs to consider the external auditor's overall audit strategy, including the planned levels of materiality and proposed resources to execute the external audit plan, and evaluate whether it appears consistent with the scope of the external audit engagement. It should also consider the seniority, expertise and experience of the external audit team.

Throughout the external audit engagement, the audit committee should challenge management and the external auditor about the:

- risks of material misstatement
- impact of changes in the business environment
- critical accounting principles
- subjective and judgemental areas of accounting
- quality of financial reporting and disclosures
- changes to accounting standards.

In the last few years, there has been a focus on enhancing the role of assurance to provide insights into the business which go beyond the effectiveness of an organisation's control environment. Technological software has progressed to analyse full populations of data which can allow for:

- the stratification of datasets to provide an informative breakdown by various subgroups

- trends across various periods, detailing effectiveness of the control environment across time
- correlation of control environment effectiveness to events occurring in the organisation (e.g. organisation restructures, implementation of new systems, departure of key personnel, etc.).

As the role of internal audit evolves over the next few years, the capability to provide assurance over a full population should be a requirement, as opposed to being a 'value add'. Substantive testing on selected samples across the year will no longer be enough to provide the board and other subcommittees with the oversight required to effectively understand and make decisions with regards to an organisation's control environment. It is, therefore, important to enquire about how internal audit is able to provide analyses over population sets of data, minimising the manual effort required to test samples. This is not to say that manual testing has no place in the future, rather, effort should be undertaken to investigate exceptions and provide thoughtful analyses from the data provided which can complement traditional auditing techniques.

ARTIFICIAL INTELLIGENCE (AI) IN ASSURANCE

AI has the ability to provide useful information to internal auditors and boards if it is used and managed well. The benefits of AI include:

- enhancing and quickening the process of data collection through machine learning, natural language processing (e.g. generative AI) and robotics
- assisting in conducting repetitive tasks and assisting auditors in the validation of information
- converting data to useful information to aid decision-making.

It will be important for internal audit and other assurance providers to leverage AI capabilities as they continue to evolve, whilst also recognising that human input is still required to assess the data and information provided.

⁸ Section 250T of the Corporations Act.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

OTHER ASSURANCE PROVIDERS

A number of different assurance providers can be used by management across its business operations. This can cover quality, clinical, training, safety and regulatory compliance type audits or reviews being routinely conducted by many businesses.

An assurance map (as described below) can be a useful tool for the board to outline the key business processes as a source of assurance, as well as expose any gaps or duplication in assurance activities. The board should be kept informed of all important findings from these assurance activities and have a formal escalation process in place. A commonly observed approach may take the form of a company policy where 'all assurance audits with a finding rated as critical must be tabled with the chair of the audit committee within one working day of identification, and all assurance reports tabled with the audit committee when final'.

ASSURANCE MAPPING

An assurance map is a structured means of identifying and mapping the main sources and types of assurance occurring throughout the organisation across the three lines of defence, and coordinating them for the best effect.

It provides great insight for boards, audit and risk committees and senior management on the extent of assurance across the three lines of defence by depicting in a clear and transparent manner:

- Key elements over which assurance is required. This will change depending on the type and size of organisation.
- The 'three lines'. The details of who provides what can vary for each organisation.
- A holistic view of assurance across the organisation.

Area	Risk	1st Line : Business Operations			2nd Line : Corporate Oversight			3rd Line: Independent Assurance			Average Level of Assurance	Desired Level of Assurance	Action
		Policy and Procedures	Management oversight & reporting	Self Assessment	Executive, Audit Committee or Treasury reporting	Independent oversight	Fraud Investigations	Internal Audit	External Audit	Other Assurance			
Finance	Risk 1	Medium assurance	Low assurance	Medium assurance				High assurance		Low assurance	Medium assurance	High assurance	Increase ↑
	Risk 2	High assurance	Medium assurance		High assurance	Medium assurance					Medium assurance	Low assurance	Reduce ↓
	Risk 3	Medium assurance	Medium assurance		Medium assurance		Medium assurance			Low assurance	Medium assurance	Medium assurance	Maintain –
	Risk 4	High assurance			High assurance				High assurance	High assurance	High assurance	High assurance	Maintain –
	Risk 5	Medium assurance	Medium assurance	Low assurance	Medium assurance			High assurance	High assurance	High assurance	Medium assurance	High assurance	Increase ↑
Operations	Risk 6	Medium assurance	Low assurance	Medium assurance				High assurance	High assurance	High assurance	Medium assurance	High assurance	Increase ↑
	Risk 7	Medium assurance	Medium assurance		High assurance	Medium assurance					Medium assurance	Low assurance	Reduce ↓
	Risk 8	High assurance	Low assurance		Medium assurance	Medium assurance				Low assurance	Medium assurance	Medium assurance	Maintain –
	Risk 9	High assurance	Medium assurance		High assurance					High assurance	High assurance	High assurance	Maintain –
	Risk 10	Medium assurance	Low assurance	Low assurance				High assurance	High assurance	Low assurance	Low assurance	Medium assurance	Increase ↑

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

- Where too little or too much assurance may be occurring based on risk appetite and hence desired level of appetite. This can be used to reallocate assurance resources as necessary for an effective outcome aligned with risk appetite.
- Duplication of assurance activities as a result of different providers/sources of assurance.

The below example assurance map extract highlights the activities that provide assurance over the key risks related to two functions. The map highlights each assurance activity's relevant strength, the type of assurance and where it sits in the 'three lines'.

The average level of assurance for each key risk is compared against the desired level of assurance (based on the risk appetite or guidance from the Audit and Risk Committee). This highlights where the level of assurance should be enhanced, or in fact decreased where it is misaligned with the risk appetite and hence assurance appetite (i.e. is over assured).

Useful resources

- Australian Government – Auditing & Assurance Standards Board, [Auditing and Assurance Standards Board](#)
- The Institute of Internal Auditors, [Welcome to IIA-Australia – Institute of Internal Auditors Australia](#)
- The Institute of Internal Auditors, The IIA's Three Lines Model, An update of the Three Lines of Defence, <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf>

For further information please contact:



Kate Shaw
 Partner, Risk Strategy
 & Technology
 KPMG Australia
kashaw@kpmg.com.au



Gary Cohen
 Director, Risk Consulting
 KPMG Australia
garycohen@kpmg.com.au

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

16. Tax Governance and Transparency

Tax governance is at the heart of tax management, and as tax reputation and sustainability principles continue to increase in relevance, so does tax governance and tax transparency. Tax governance can and should be considered together with the performance of tax functions in support of business objectives.

In this chapter

- Overview of Tax Governance
- Governance over third-party data
- Tax Transparency and Reporting Measures
- Director's Responsibilities
- Recent Developments and Trends in the Market
- Future Direction

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Is there a formalised tax control framework/policy setting out tax risk management and governance that has been endorsed by the Board? Are we conducting regular reviews to validate the effectiveness of our tax governance framework?
2. Does the framework/policy include the organisation's Tax Risk Appetite in relation to strategic and day to day risk? How is the Tax Risk Appetite documented and communicated?
3. Is the tax control framework/policy published internally and externally? Are measures in place to ensure it is properly understood?
4. Is the tax risk management escalation model formally documented? This would involve tax risks related to significant transactions or events being identified, assessed and escalated (including when to seek external tax advice).
5. In relation to Question 4, is it clear when the Board should be involved on tax risks?
6. Are the roles and responsibilities/delegation for tax risk management and governance documented in the Board/ Sub-Committee charters?
7. Does the company have a Board skills and competency matrix covering tax?
8. Is a tax briefing included in the tax induction programme for new Board directors?
9. Is the Board regularly informed on tax compliance, legislative developments that may have an impact on the organisation and how tax issues and risks are trending (e.g. tax risk register /enterprise risk register that includes tax risk)?
10. Is periodic internal control testing conducted to assure the Board that the internal control framework is robust enough to effectively manage tax risk?
11. Are directors aware of their personal liability exposures for unpaid Pay as You Go (PAYG), Goods and Services Tax (GST) and Superannuation Guarantee Charge (SGC)?
12. Has the potential impact of the mandatory tax transparency reporting requirements here in Australia and globally been assessed, and if relevant, has a governance model established to be comfortable with the information to be made public?
13. For groups with an international presence, has the evolution in global trends including Organisation for Economic Cooperation and Development (OECD) Base Erosion and Profit Shifting (BEPS) Pillar 2 and the inclusion of tax in sustainability reporting in the EU been considered? How are we preparing for the implementation of the OECD BEPS Pillar 2, including the global minimum tax and its potential impact on our effective tax rates?
14. Is the tax function included in business wide Environmental, Social and Governance (ESG) initiatives? Changes in supply chains, new investments, workforce, sustainability reporting and government policy incentives can have tax implications.
15. As finance, tax and other functions utilise generative AI and related technologies, what governance is in place around their usage to support compliance with regulatory requirements?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- Tax risk management and governance framework is not formalised/established.
- Tax strategy/policy/framework is not reviewed regularly and/or endorsed by the Board.
- Tax Risk Appetite is not incorporated in the overarching risk appetite statement.
- Tax risk management escalation is not formally documented or established.
- Roles and responsibilities for tax governance and risk management are not formalised.
- The Board is not informed of tax risks and taxation developments.
- Internal control framework is not tested periodically.
- Lack of a governance model for managing public tax transparency measures.
- A strategy for new and emerging tax transparency developments, such as OECD Pillar 2 or other global tax initiatives not in place.
- Over-reliance on manual processes for tax compliance, increasing the risk of errors and inefficiencies.
- Lack of policies for seeking independent advice on high-risk or complex tax transactions.
- Failure to address the integration of tax considerations into ESG strategies and reporting.
- Is there an over-reliance on third-party data for tax compliance and reporting, potentially leading to inaccuracies, data security risks, and compliance issues if the data is not accurate, reliable, or secure?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

OVERVIEW OF TAX GOVERNANCE

Tax governance involves establishing clear processes and procedures, supported by robust controls, to achieve business objectives and ensure compliance with tax obligations. The foundation of a successful tax governance framework includes setting a tax strategy, implementing processes and controls, and taking proactive measures to bring it to life. Establishing the right operating model for your tax function is key.

In Australia, the significance of demonstrating tax governance measures has seen a notable shift. The Australian Taxation Office (ATO) through its Justified Trust (JT) methodology, has had a substantial impact, particularly through its Top 100 and Top 1000 compliance program as well as certain Private Group initiatives. 'Justified Trust', an OECD concept, aims to strengthen community confidence that taxpayers are paying the correct amount of tax. Additionally, in 2023 an updated version of the G20 / OECD Principles of Corporate Governance (Principles) was endorsed by G20 Leaders. The document addresses various corporate governance matters, emphasizing the importance of tax governance in several areas.

ATO focus

The ATO has released the Tax Risk Management and Governance Review Guide (**ATO Guide**)¹ establishing a series of expectations of taxpayers in the design and operation of tax risk management and governance. In addition to this, the ATO has released the GST Governance, Data Testing and Transaction Testing Guide (**ATO GST Guide**)² which goes into more detail with respect to GST related controls. More recently, in June 2024, the ATO released a Top 1,000 GST Analytical Tool (**GAT**) and data testing guide to provide industry guidance that the GAT is used to ensure the right amount of GST is paid. The benefits of establishing tax governance include:

- Increased comfort that tax outcomes are being consistently achieved within a defined risk appetite, with fewer surprises.
- Ensuring the Board is informed of tax risks and regularly updated on how tax issues and risks are trending, providing a framework for effective tax decision-making.
- Saving time through greater clarity in responsibilities and the procedures to occur across organisations.
- Streamlined and standardized tax processes across the organisation to reduce the duplication of efforts and increase efficiency.
- Addressing key person risks and saving time having in place documentation of the tax governance framework and key processes, controls and policies when team members change.
- Providing a structured approach to avoid complacency and identify process and other improvements.
- Providing a structured approach to identify the needs and build the business case to address tax data and tax technology needs as regulators globally invest in their own data technologies.
- Demonstrating purpose and care towards internal and external stakeholders, creating a positive legacy.

GST

GST is assessed separately and receives its own tax governance rating, distinct from the income tax rating. By having a separate GST tax rating, organisations are required to more closely consider their GST compliance and address any specific issues related to GST reporting.

¹ Australian Taxation Office (ATO), Tax risk management and governance review guide, <https://www.ato.gov.au/Business/Large-business/In-detail/Key-products-and-resources/Tax-risk-management-and-governance-review-guide/>

² ATO, GST Governance, Data Testing and Transaction Testing Guide, <https://www.ato.gov.au/law/view/document?DocID=JTR/GST-Governance&PIT=99991231235958>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

GOVERNANCE OVER THIRD-PARTY DATA IN THE INVESTMENT INDUSTRY RELATED SECTORS

The ATO has issued a supplementary guidance³ for third-party data controls specifically applying to *large superannuation funds, managed funds and insurance companies* (entities). Entities will need to adopt the principles-based approach below to determine appropriate controls that are fit for purpose:

Principle	ATO Supplementary Guide <i>Governance over Third-Party Data</i>
Principle 1: Roles and Responsibilities	The entity needs to understand the roles and responsibilities of outsourced service providers.
Principle 2: Tax policy in accordance with the law	The entity needs to be satisfied that the tax policies of the outsourced service providers are prepared in accordance with the tax law.
Principle 3: Returns and tax outcomes properly reflected in tax reporting	The entity needs to be satisfied that the tax policies of the outsourced service providers are reflected in the tax reporting relied upon by the entity.
Principle 4: Independent assurance	The entity needs to seek assurance from independent parties in relation to the accuracy of the data received and processed by outsourced service providers. Testing of tax specific controls not already covered in existing testing programs.

³ ATO, Governance over third-party data, Supplementary guide for large superannuation funds, managed funds and insurance companies on third-party data tax controls [governance-third-party-data.pdf](#)

Outsourced service providers including custodians and administrators collate and present third-party data in tax reports, relying on data, systems and/or the software of these service providers. Entities relying on third-party data from outsourced service providers should document how data integrity is assessed with respect to the underlying data feeding into tax reporting obligations and the information contained in these returns.

The Trustees, Board or relevant Board-endorsed sub-committee will need to ensure the systems and processes to validate data accuracy are developed in line with the organisation's tax risk management framework.

Until 1 July 2024, a transition or implementation phase was in place to allow entities time to develop processes and procedures and implement tax controls for tax governance over third-party data. Since 1 July 2024 however, the ATO have started to rate separately taxpayers on third-party data reliance governance in addition to the other tax governance ratings.

TAX TRANSPARENCY AND REPORTING MEASURES

Australian Public Companies

For Australian Public Companies there are new disclosure requirements in the financial statements regarding the tax residency of subsidiaries for reporting periods starting on or after 30 June 2024. For multinational groups, in addition to the tax technical assessment of tax residence, appropriate governance measures need to be in place to reinforce the principles and support the operating measures for tax residency assessments.

Mandatory Public Tax Transparency

Australian legislation is now in effect requiring mandatory public reporting of taxes paid for groups with an annual global turnover of A\$1 billion or more. This new tax transparency measure (Australian public country-by-country reporting (**CbCR**)) significantly increases the amount of tax information that multinational enterprise (**MNE**) groups must disclose to the public.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The Australian public CbCR rules are broadly based on the quantitative reporting aspects of Global Reporting Initiatives' (GRI) Sustainability Reporting Standards, in particular GRI 207-1 and 207-4. In-scope groups will generally be required to provide the following information, which will be made publicly available on the Australian government website:

- Names of each entity in the CbCR group;
- Description of the CbCR group's approach to tax; and
- Quantitative tax information for the income year shown for the relevant jurisdictions in which the CbC reporting group operates. This may be required to be aggregated or disaggregated for disclosure purposes. A list of 'specified countries' has been determined for which disaggregated information must be disclosed.

The CbC reporting parent will be required to report periods that start on or after 1 July 2024, with the rules requiring submission of the select tax information within 12 months of the end of the reporting period. This means that for 30 June 2025 reporting period, the tax information will need to be provided to the Commissioner for publishing by no later than 30 June 2026.

The rules will broadly apply to both Australian headquartered MNE groups with global consolidated income of more than A\$1 billion in the prior year and foreign owned MNE groups with Australian permanent establishments with at least A\$10 million aggregated Australian-sourced income in the current year.⁴

This is in line with emerging global requirements such as the mandatory EU public CbCR rules, applying to financial years starting on or after 30 June 2024. We note there are commonalities and points of distinction between the Australian and EU CbCR rules. Australian MNE groups trading in the EU (through EU subsidiaries or branches) with total consolidated revenue of over €750 million may be subject to both compliance requirements.⁵

⁴ KPMG, 2024, Australian public country-by-country reporting, [Australian public country-by-country reporting – final legislation passes](#)

⁵ KPMG, Country-by-Country Reporting <https://kpmg.com/xx/en/home/services/tax/regional-tax-centers/eu-tax-centre/country-by-country-reporting.html>

Furthermore, existing OECD CbC obligations will remain, meaning that MNE groups will need to prepare and finalise their existing CbC reporting requirements in parallel with the new public CbCR measures.

Voluntary Tax Transparency Code (TTC)⁶

The TTC has been in place since 2016, with over 200 Australian based and inbound groups now signatory to the TTC. The TTC, a voluntary model, was developed by the Board of Taxation. As of now, in the light of the new mandatory public CbCR, the Board of Taxation are undergoing a consultation process to update the TTC. Based on the consultation draft the direction of travel is to leverage other aspects of GRI 207 for those who voluntarily want to go beyond the mandatory public CbCR rules mentioned above or are not subject to those rules. Organisations should monitor the status and consider the application of any revised TTC.

Tax in sustainability reporting

In addition to tax specific transparency reporting, tax considerations may become relevant for new sustainability reporting requirements being implemented both in Australia and globally. As sustainability reporting evolves, it is essential to integrate tax governance and transparency to ensure comprehensive and accurate disclosures.

DIRECTOR'S RESPONSIBILITIES

The ATO Guide sets out the responsibility of the Board to oversee and monitor an organisation's governance processes and risk management frameworks with Management responsible for day-to-day operation.

In addition, the Director penalty regime prescribes personal liability if a company does not meet its PAYG withholding amounts, GST or SGC obligations.⁷ The Director penalty regime will not affect directors if they ensure their company complies with its PAYG withholding and SGC obligations.

⁶ Corporate Tax Transparency Code and Register | Board of Taxation (taxboard.gov.au)

⁷ ATO, Director Penalties, <https://www.ato.gov.au/businesses-and-organisations/hiring-and-paying-your-workers/engaging-a-worker/in-detail/director-penalty-regime>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

RECENT DEVELOPMENTS AND TRENDS IN THE MARKET

ATO perspectives

In response to ATO guidance on tax risk management and governance, many groups have enhanced their tax governance measures. As an example, more recently almost half of the Top 100 and Top 1000 committing to ongoing testing of tax controls which is a significant increase from just a few years ago. ATO expectations continue to increase and organisations are encouraged to regularly assess and enhance their tax governance measures as required.

Recently the ATO has recalibrated metrics used to determine the Top 1,000 taxpayers under a 'differentiated approach'. Top 1,000 taxpayers are divided into two groups, significant and general pool taxpayers, those with total business income over \$1 billion and over \$350 million representing the top 30% and bottom 70% of Top 1,000 taxpayers respectively. For taxpayers receiving a stage 2 or stage 3 tax governance rating in a previous review, the ATO may exercise discretion to adopt a 'lighter touch', potentially reducing the quantum of tax governance questions. This presents an incentive to achieve a stage 2 or stage 3 tax governance rating.

Pillar 2 global minimum tax

The Australian Government has enacted legislation introducing a 15% global minimum tax and an Australian domestic minimum tax for larger MNE groups. This applies to MNEs with consolidated annual revenue of at least €750 million (approx. A\$1.2 billion) for at least two of the last four years.

The new Australian rules include:

- **Income Inclusion Rule (IIR)** – allows Australia to impose a top-up tax on Australian parent entities where the group's effective tax rate in another jurisdiction is below 15%;
- **Undertaxed Profits Rule (UTPR)** – acts as a backstop, enabling Australia to apply a top-up tax on Australian entities where the group's effective tax rate in another jurisdiction is below 15% and where low-taxed profits are not captured by an IIR; and

- **Domestic Minimum Tax (DMT)** – provides Australia the ability to claim primary rights to impose top-up tax over any low-taxed profits in Australia, in priority over the IIR and UTPR.

The start date for these measures is income years on or after 1 January 2024 for the IIR and DMT, and income years on or after 1 January 2025 for the UTPR. The implementation of these rules may impact tax reporting disclosures.

Capital allowances

The ATO appears to be increasing its focus on capital assets, emphasizing the need for appropriate governance to manage capital allowances accurately and transparently. The ATO's considers⁸ both the systems and governance processes adopted, as well as the supporting evidence provided. The common issues identified include inadequate documentation to support self-assessed effective lives, disclosure errors in tax returns and incorrect asset classification.

GST Supplementary return

The ATO has introduced the new GST Supplementary Return.⁹ It requires businesses to make specific assertions regarding the accuracy and completeness of their GST data, the effectiveness of internal controls over GST reporting, and their compliance with GST law. This initiative aligns with the ATO's focus on promoting governance and risk management in tax reporting.

The return is mandatory for certain large market taxpayers, those in the Top 100 and Top 1,000 populations that have received a GST tax governance rating from the ATO, and serves as an additional assurance measure aligned with the Justified Trust program.

⁸ ATO findings report: Top 1,000 income tax assurance | Australian Taxation Office
⁹ Supplementary annual GST return 2025 | Australian Taxation Office; New GST return puts the spotlight on assurance review commitments - KPMG Australia | Content Plus

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Reporting and value creation

The increasing amounts of external reporting on tax, including mandatory tax transparency, highlights the important role tax functions play in meeting business and reputation objectives.

Together with operational imperatives in terms of costs, the constantly evolving tax landscape requires regular consideration of how tax functions are managed.

This can be in terms of improving reporting on tax priorities and outcomes to senior management and the board, maximising the use of technology to improve efficiencies, and how tax has a role in value creation for the business. Such value creation can be in support of business teams and priorities, appropriate tax input on major transactions, ensuring appropriate coverage of grants and incentives which can have a tax flavour, and appropriate coverage of issues that have some tax implications – such as employment taxes.

Another emerging topic for institutional and retail investors is responsible investing from a tax perspective. For instance, according to a survey¹⁰ by the Responsible Investing Association, a significant portion of consumer investors want to avoid investments in companies that don't pay a fair amount of tax. This rise of socially responsible investment is demonstrated by investors becoming increasingly aware that aggressive tax planning carries reputational risks and conflicts with having a responsible tax risk appetite. Institutional investors are increasingly considering tax governance and related attributes in target companies.

FUTURE DIRECTION

Regulators are calling for increased sophistication of an organisation's data level controls, and in the level of detail and consistency of framework and process controls. The tax governance enhancement opportunity here is to embed more controls to boost contemporaneous documentation and enhancement of the evidence of the governance process.

The Global Anti-Base Erosion Model Rules (**GloBE Rules**) in relation to Pillar 2 is another area that now requires greater tax governance emphasis. MNEs subject to the GloBE Rules are obliged to file a copy of the GloBE Information Return (**GIR**) to their local tax administrator. The GIR is a key administrative document to notify tax administrations that an MNE group has constituent entities in its jurisdiction and will provide information used to calculate any potential top-up tax payable. The tax governance enhancement opportunity here is to create end-to-end documented procedures to assist clients with the annual process of preparing, reviewing and filing the GIR.

For Directors, it is essential to ensure that your organisations adapt to these rules efficiently, minimising the risk of non-compliance, and making the most of any strategic opportunities that enhanced governance may provide.

¹⁰ Benchmark Report - Responsible Investment Association Australasia (RIAA)

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- *Tax Risk Management and Governance Review Guide*, <https://www.ato.gov.au/Business/Large-business/In-detail/Key-products-and-resources/Tax-risk-management-and-governance-review-guide/>
- GST Governance, Data Testing and Transaction Testing Guide, <https://www.ato.gov.au/law/view/document?DocID=JTR/GST-Governance&PiT=99991231235958>
- Top 1,000 GAT and data testing, <https://www.ato.gov.au/businesses-and-organisations/corporate-tax-measures-and-assurance/large-business/top-1000-gat-and-data-testing>
- Governance over third-party data, <https://www.ato.gov.au/law/view/document?DocID=JST/Governance-third-party-data&PiT=99991231235958>
- Director Penalty Regime, <https://www.ato.gov.au/businesses-and-organisations/hiring-and-paying-your-workers/engaging-a-worker/in-detail/director-penalty-regime>
- KPMG, 2024, Australian public country-by-country reporting,
- Australian public country-by-country reporting – final legislation passes
- KPMG, EU Public CbyC implementation tracker
- Country-by-Country Reporting
- KPMG, Pillar 2 reporting
- Pillar Two top-up taxes in financial reports

For further information please contact:



Phil Beswick

Lead Partner, Tax Governance
KPMG Australia
pbeswick@kpmg.com.au

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

17. Risk Management

Ultimate responsibility for risk lies with the board. Consequently, risk management is a focus of the board and executive management.

In this chapter

- Key concepts
- ASX Corporate Governance Principles and Recommendations
- AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines
- Risk and strategy
- Risk governance
- Risk culture
- Risk management policy
- The benefits of enterprise-wide risk management
- Risk appetite
- Crisis management
- Business continuity
- Organisational roles

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Are the relevant roles and accountabilities for governance, risk and compliance properly formalised and documented with appropriate interfaces in place?
2. Does the board share a common view of what the risk appetite is, such that this may be consistently applied in decision-making?
3. Are assurance activities based on appropriate and robust structures and aligned to the risk profile and appetite of the organisation?
4. Do board members appreciate the potential consequences of serious governance, risk and compliance failures?
5. Is sufficient focus paid to both non-financial and financial risks in discussions?
6. Are there early warning systems and leading indicators in place to alert the board and senior management to emerging risks?
7. Is there integration and alignment of risk management with strategic direction and planning?
8. Is the board aware of how management is using risk information and the risk appetite established by the board to inform decision-making?
9. How are missed opportunities, or realised risk events, identified and discussed?
10. Does the board provide oversight on plans for crisis management and business continuity?
11. Is the board establishing the 'tone at the top' to reinforce and promote a risk-aware culture?
12. Has the board set a clear direction for risk culture and the expectations for ongoing measurement and reporting?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- Limited time is given to discussing risk at board and audit and risk committee forums.
- Risk management is not connected to corporate strategy.
- There is a disconnect between risks discussed at a board level (strategic risks), those reported in the annual report and the operational risks on which management focus. Risk management is positioned as a compliance and backroom exercise.
- Risk reporting and risk management plans are not challenged at board level.
- A strong risk culture is not embedded throughout the organisation.
- A risk appetite statement has not been developed and communicated.
- Risk issues are being brought to the attention of the board through media and stakeholders rather than management.
- The board cannot clearly describe its risk management processes.
- The audit and risk committee(s) does not meet or report to the board on a regular basis.
- Focus is unduly placed on one kind of risk (eg financial risks over non-financial risks or safety risks over operational risks) without good reason.
- Accountability for risk identification, management and treatments is unclear and discussion on how risks should be managed often goes unresolved.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

KEY CONCEPTS

Risk is 'the effect of uncertainty on objectives' (see AS/NZS ISO 31000:2018).

Risk management is the culture, processes and structures that are directed towards the effective management of potential opportunities while managing the potential adverse effects.

Enterprise-wide risk management is an organisation-wide approach to the identification, assessment, communication, and management of risk in a cost-effective manner – a holistic approach to managing risk.

Risk governance incorporates the processes necessary to bring reliable risk management information to the attention of the board.

Effective boards consider the robustness of risk governance systems, understand how they work, and to what extent they have the capacity to provide them with assurance.

ASX CORPORATE GOVERNANCE PRINCIPLES AND RECOMMENDATIONS

Recognising and managing risk is a critical role of the board and management. Failure to do so may adversely impact on security holders and all other stakeholders.

Principle 7 of the ASX Principles recommends that companies should establish a sound risk management framework, and periodically review the effectiveness of that framework.¹ It makes the following recommendations:

- *Recommendation 7.1* – The board of a listed company should have a committee or committees to oversee risk (this may be a standalone committee or combined with the audit committee).

- *Recommendation 7.2* – The board or a committee of the board should review the entity's risk management framework at least annually to satisfy itself that it continues to be sound; and disclose, in relation to each reporting period, whether such a review has taken place.
- *Recommendation 7.3* – A listed company should disclose if it has an internal audit function, how the function is structured and what role it performs; or if it does not have an internal audit function, that fact and the processes it employs for evaluating and continually improving the effectiveness of its risk management and internal control processes.
- *Recommendation 7.4* – A listed company should disclose whether it has any material exposure to environmental or social risks and, if it does, how it manages or intends to manage those risks.

AS/NZS ISO 31000:2018 RISK MANAGEMENT – PRINCIPLES AND GUIDELINES

AS/NZS ISO 31000:2018 (ISO 31000) sets out the principles for effective risk management and the key building blocks for an organisation to develop and embed a comprehensive risk management framework. ISO 31000 standard is the recognised industry standard for managing risks and is commonly applied across private and public sector organisations in Australia. The objective of ISO 31000:2018 is to assist organisations to develop an enterprise-wide risk management strategy to effectively identify and mitigate risks and achieve organisational objectives. In order to achieve this, it adopts a strategic focus and emphasises the role of senior management and the integration of risk management across the organisation. Interestingly, ISO 31000 defines risk as 'the effect of uncertainty on objectives' and as such does not focus purely on the downside of risk in the way that traditional risk management historically has. This aligns with the strategic focus of the standard whereby if an organisation is able to proactively manage its risk profile, risk may in fact represent an opportunity (or upside).

¹ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Principle 7.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

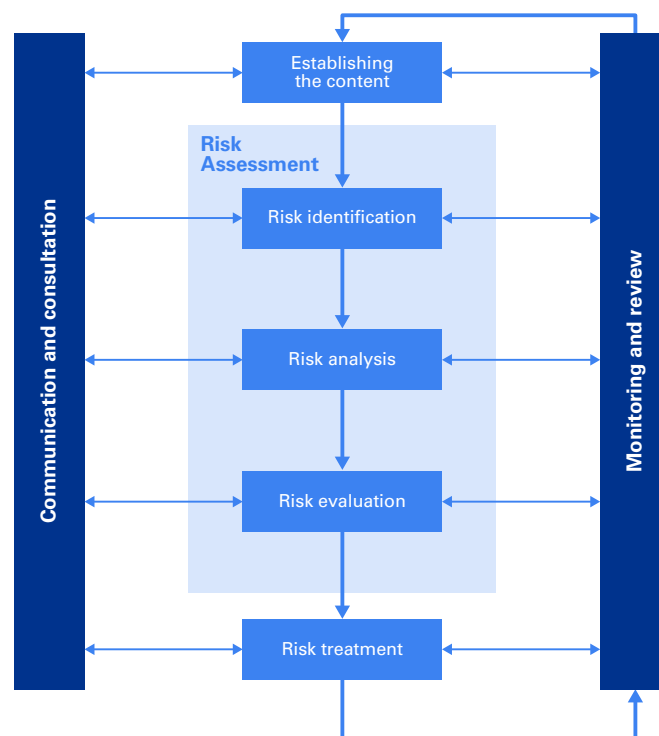
18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The following diagram summarises the approach to risk management described in ISO 31000.



ISO 31000:2018

Whilst not mandatory, the principles and guidelines outlined in ISO 31000 are considered to be best practice from a high level to facilitate proactive risk management. All directors should understand these basic principles and, more importantly, how to ensure that they are being implemented effectively by management.

RISK AND STRATEGY

Risk and strategy are essentially two sides of the one coin, with the development of strategy subject to the risks that threaten its achievement. Despite the benefits of integrating these two key processes, many organisations struggle to do this and will typically identify the risks to their strategy after the strategy has been developed, rather than using an understanding of the risk environment to inform the strategy and then identifying risks to the strategy thereafter.

Experience suggests that organisations that make risk management an integral part of their strategy are more resilient in dealing with adverse events and uncertainty. Poor management of material business risks has been widely recognised as one of the key contributors to corporate failures during the global financial crisis (GFC). The latter provided useful lessons that listed entities can draw on to improve risk management and risk disclosures to stakeholders.

RISK GOVERNANCE

Risk governance incorporates the processes and supporting systems necessary to bring reliable risk management information to the attention of the board. It encompasses the overarching risk management structure to facilitate the management of risks across an organisation. It includes the formal policies and procedures in place for key risk areas, disciplines and reporting. The increasing availability and options for integrated governance, risk and compliance (GRC) systems has seen Australia begin to embrace the power of risk management technology at a faster pace which is providing an effective and efficient solution for risk governance.

Many audit committees today have oversight responsibility for the company's enterprise risk management process, as well as other major risks facing the company – including financial, operational, cyber security, IT, legal and regulatory compliance. Other organisations establish a separate risk committee to focus specifically on risk identification and management oversight issues (this is discussed further in [Chapter 11](#)).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

RISK CULTURE

Establishing organisational culture is the responsibility of the board, and this includes developing, communicating and 'living' the organisation's risk management culture.

Culture can be difficult to define, however, it is often thought of as 'the way we do things around here'. Whilst an organisation might have a best practice set of policies and processes in place to manage key risk areas of the business, they will be ineffective if they are not adhered to by staff.



FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Increasingly, regulators such as ASIC are interested in corporate culture and the impact that it has on business conduct and, therefore, financial consumer trust and confidence.² Whilst culture cannot be regulated, conduct can. In the context of risk, the conduct of employees is significant, as employee behaviours can quickly impact on financial performance and the organisation's reputation.

Risk management implementation not only requires significant effort, but also the creation of a risk management culture that is committed to managing risk within the boundaries defined by the board. The board must set the 'tone at the top', whilst management sets the 'mood in the middle'. Ensuring these behaviours are consistent requires a proactive approach. Key actions to establish a common risk culture include:

- communicating the board's vision, strategy, policy, responsibilities and reporting lines to all employees and stakeholders
- developing a clear risk appetite statement that communicates the end vision and benefits, and the acceptable thresholds within which decisions can be made by the business
- establishing a control environment that assigns responsibilities for risk management, and that has an effective and consistent measurement and accountability framework
- implementing training programs for risk management, that includes identifying and training 'risk champions', and developing a knowledge-sharing system
- communicating success stories and identifying quick wins.

RISK MANAGEMENT POLICY

A listed entity established in Australia is required under the Corporations Act to include a discussion in the operating and financial review, contained in its directors' report of the main internal and external risk sources (including environmental and sustainability risks) that could adversely affect the entity's prospects for future financial years.³

² Refer to speeches by Greg Medcraft, John Price of ASIC regarding culture and ethics, available at <https://asic.gov.au/regulatory-resources/corporate-governance/directors-and-corporate-culture/>

³ Corporations Act 2001, s 299A(1) and ASIC Regulatory Guide 247 (RG247) – Effective disclosure in an operating and financial review.

If a significant risk event occurs, the company may also have to disclose the occurrence and its impact pursuant to its continuous disclosure obligations under the Listing Rules.⁴

Risk management policies should reflect the company's risk profile and should clearly describe all elements of the risk management and internal audit function.⁵ The policy should be an instrument to communicate the company's risk-management approach and should include, at a minimum:

- a definition of 'risk' and 'risk management' relative to the organisation
- goals and strategies for risk management
- the organisation's risk appetite/tolerance
- how risk management targets will be measured
- accountabilities for risk management.

THE BENEFITS OF ENTERPRISE-WIDE RISK MANAGEMENT

The elements that comprise an ERM framework are defined in the graphic below. Potential benefits of having an integrated ERM framework include:

- better informed decisions
- greater management consensus
- increased management accountability
- greater ability to meet strategic goals
- reduced earnings volatility
- better allocation of resources, which may lead to increased profitability
- ability to use risk as a competitive tool
- more accurate risk adjusted pricing
- better contingency planning
- improved crisis response.

⁴ See Chapter 7 – Accountability to Shareholders.

⁵ *ibid.*

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ELEMENTS OF A RISK MANAGEMENT FRAMEWORK

	Risk Strategy & Appetite	Alignment/Conscious decision to use risk management to enable the achievement of business plans, goals and strategic objectives. It includes a risk appetite statement supported by risk tolerances, limits and associated breach protocols to control risk levels throughout the organisation.
	Risk Governance	A structure through which an organisation directs, manages and reports its risk management activities. It encompasses clearly defined roles and responsibilities, decision rights, the risk governance operating model, and reporting lines.
	Risk Culture	Values and behaviors present throughout an organisation that shape risk decisions. Risk culture influences the decisions of management and employees, even if they are not consciously weighing risks and benefits. A strong risk culture helps to encourage strategic decisions that are in the long-term best interest of the organisation, its shareholders and employees.
	Risk Assessment & Measurement	The activities in place that allow an organisation to identify, assess and quantify known and emerging risks. The risk assessment and measurement processes allow organisations to consider the extent to which potential events may have an impact on achievement of objectives. It encompasses qualitative and quantitative approaches, processes, tools and systems that organisations develop and implement to identify, assess, and measure risks.
	Risk Management & Monitoring	Management's response to manage, mitigate, or accept risk. Risk management efforts create value through the use of risk and control information to improve business performance across the enterprise. Systematically monitoring the identified risks and management activities against established metrics permits timely proactive response where warranted. Management designs activities to assure stakeholders that risk management activities and controls are effective in managing risks that could have an impact on achievement of objectives (i.e. Integrated Assurance).
	Risk Reporting & Insights	Reporting of risk and related information (e.g. mitigation activities) provide genuine insight into the strengths and weaknesses of risk management activity. Disclosure of risk management information to key stakeholders also supports the decision-making processes. Effective risk reporting enhances the transparency of risks that could have an impact on achievement of objectives in a timely manner.
	Data & Technology	Management of risk data that can be translated into meaningful risk information for stakeholders. It includes the development and deployment of risk management tools, software, databases, technology architecture, and systems that support risk management activities.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

RISK APPETITE

Risk appetite is the amount of risk, at a broad level, that an organisation is willing to accept in pursuit of value. It will reflect the risk management philosophy and the organisation's capacity to take on risk. It is based on strategic objectives and stakeholder demands. The notion of risk appetite can add discipline and focus when responding to an uncertain and constantly shifting risk environment. A risk appetite statement can provide a decision-making framework for the strategic and operational handling of risk. As the appetite may vary across different parts of the business and different risk types, it is important that the appetite for each area and risk type is specified. For example, the risk appetite for health, safety and wellbeing related risk is most commonly low, however, the appetite for innovation is high (so as to allow for a safe-to-fail and innovative culture). This then drives the resourcing into the control frameworks for each area accordingly.

Risk appetite, if embedded and used well, can support resource reallocation and cost reduction where needed. Setting key risk indicators aligned to the risk appetite enables proactive risk management through early warning signals being monitored and reported.

CRISIS MANAGEMENT

Companies should have crisis management plans in place. Such plans should include reference to the board's role during a crisis and should be considered as part of a board's risk management responsibility. Boards should insist that crisis management plans contain a robust communications element.

Without effective communication, companies may inflict additional damage on themselves including:

- losing control of the communications process
- allowing facts to be displaced by rumour and speculation
- reputational harm
- putting employee morale and trust at risk
- alienating shareholders, customers, suppliers and other stakeholders.

Contemporary risk management frameworks, including crisis management plans, should incorporate the mitigation of social media as a key function. Boards and senior management need to be prepared to manage and respond to social media.

BUSINESS CONTINUITY

Planning for a disaster is considered essential practice as all businesses face the risk of a serious event occurring that can damage the organisation's ability to continue operating.

Business continuity management focuses on an organisation's responsiveness to an organisational or external crisis that puts its ongoing operation at risk. The aim is to foster and develop preparedness for all types of events that may significantly affect an organisation and enable a company to respond and resume normal business operations after they occur.

The ultimate goal of business continuity is to develop a response to events to enable the organisation to maintain its most critical operations, and survive all but the most extreme forms of operational disruption. The key elements of effective business continuity planning are flexibility and simplicity.

A well-prepared organisation will be able to make the right decisions at the right time, based not on rigid instructions contained in a detailed manual, but on tried and tested alternative ways of working.

These arrangements must:

- be integrated into everyday business
- look inside as well as outside the organisation
- be understood by employees and stakeholders
- be regularly and effectively tested to ensure they remain relevant.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ORGANISATIONAL ROLES

The board

The board is ultimately responsible for risk management. The board:

- approves the organisation's risk appetite as recommended by the audit and risk committee
- must regularly review and approve the organisation's risk management policy, and maintain oversight of the policy
- approves the risk management framework for the organisation
- receives regular updates about key risks, changes in risks and emerging risks from the audit and risk committee
- establishes board subcommittees (audit and risk committee) and evaluates committee performance.

Chief risk officer

It is common for organisations to have appointed a chief risk officer (CRO) or risk manager. The existence of a CRO centralises risk management, but also brings several other benefits. One is to understand the relationship between risks within separate business units that might not have been apparent before. This is becoming more important given the increasing diversity and complexity of global businesses in which a risk that appears acceptable to the manager of an individual business unit may be inappropriate from the point of view of the enterprise as a whole. Using a comprehensive risk matrix, CROs can identify such linkages across the business and manage them more effectively.

Another important way CROs can benefit the business is by enabling the organisation to make decisions based on a better appreciation of the relationship between risk and reward. CROs are most effective when they provide the board with a clear vision of where enterprise risks lie, help define a policy for distributing and offsetting those risks, and work to communicate that vision so that individual managers understand and support it. The CRO provides a framework for risk management while decisions on what is acceptable risk fall to managers and employees in the frontline of the business.

Risk management committee

The ASX Principles recommend that the board of a listed entity has a risk committee in place to oversee risk and the risk management committee should review the entity's risk management framework at least annually (with disclosures as to whether such a review has taken place).⁶ Many companies have established risk management committees, or have a combined audit and risk committee. This committee acts as an efficient mechanism for focusing the company on appropriate risk oversight, risk management and internal control. A risk committee can be an efficient and effective mechanism to bring the transparency, focus and individual judgement needed to oversee a company's risk management framework. For companies that do not possess a risk management committee (e.g. in the case of smaller boards where the same efficiencies may not necessarily be derived from a formal committee structure), board processes should raise the issues that would otherwise be considered by a risk management committee.

Generally the risk management committee will have a key role in the governance of risk and compliance, including:

- oversight of the risk management framework and its implementation
- considering and challenging risk reporting
- oversight of the compliance framework
- considering and directing management's response to key risk issues.

The commentary to Recommendation 7.1 of the ASX Principles lists those matters for which the risk committee should be responsible for making recommendations to the board.⁷

⁶ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Recommendations 7.1 and 7.2.

⁷ Refer also [Chapter 11](#) – Board Committees.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

• GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- ASIC, 2016, Good corporate culture, values and ethics, <http://asic.gov.au/about-asic/media-centre/speeches/good-corporate-culture-values-and-ethics/>
- ISO 31000:2018, Risk Management – Principle and Guidelines
- KPMG, 2019, Risk Reimagined, <https://assets.kpmg/content/dam/kpmg/au/pdf/2019/risk-reimagined-seize-opportunity-in-risk.pdf>

For further information please contact:



Kate Shaw
 Partner, Risk Strategy
 & Technology
 KPMG Australia
kashaw@kpmg.com.au



Gary Cohen
 Director, Risk Consulting
 KPMG Australia
garycohen@kpmg.com.au

Governance Oversight

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

18. Environmental, Social and Governance (ESG)

The most significant development has been the establishment of Australia's sustainability reporting framework with *Treasury Laws Amendment (Financial Market Infrastructure and Other Measures) Act 2024* receiving Royal Assent in September 2024. The Act requires relevant entities to disclose their climate-related plans, financial risks and opportunities in accordance with Australian Sustainability Reporting Standards (ASRS) developed by the Australian Accounting Standards Board (AASB).

This chapter has two sections:

1. Australian Sustainability Reporting Standards (ASRS) Framework

This section focuses on the new regulatory reporting requirements.

2. ESG Considerations

This section considers broader ESG risk areas.

In this chapter

- The Australian Sustainability Reporting Standards
- ASIC Regulatory Guide 280: Sustainability Reporting
- Strategy
- Identifying material risks
- KPIs and targets
- Drivers
- The sustainability reporting context

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

Australian Sustainability Reporting Standards (ASRS) framework:

Governance and oversight

1. Is the company captured under the ASRS, and if yes, when is the first reporting date?
2. Does the company have a plan in place to satisfy the disclosure requirements ahead of the first year's reporting? Are the directors being informed of progress of some of the more challenging disclosure areas, which include Scope 3 GHG emissions, climate scenario analysis and forward-looking qualitative and quantitative climate risks and opportunities disclosures?
3. Are directors adequately informed about their responsibilities, including the directors' duties?
4. Has the company taken 'reasonable steps' to ensure compliance with reporting standards during the transitional period?
5. Are directors aware of which statements are protected under modified liability provisions – and which are not?
6. Is there a designated executive and/or committee responsible for ASRS reporting?
7. Does the board have confidence they have the skills to critically assess the ASRS disclosures and challenge management where necessary?
8. Has the company established clear governance structures to oversee climate-related risks and opportunities?

Strategy and risk management

1. How are climate-related risks and opportunities integrated into the overall business strategy?
2. Has the company identified and assessed all material climate-related financial risks and opportunities?
3. Is the company using a scenario analysis to evaluate climate resilience under different temperature pathways (e.g. 1.5°C and >2.5°C)?
4. Does the company have a transition plan in place to address climate-related risks and opportunities?

Reporting and assurance

1. Has the company implemented process, systems and controls to ensure the accuracy and completeness of sustainability disclosures?
2. Are disclosures supported by reasonable assumptions and data, including for Scope 3 emissions and forward-looking statements?
3. Is the company maintaining sustainability records for at least seven years, as required?
4. Is the company prepared for the phased introduction of assurance requirements, as established by the Australian Auditing and Assurance Standards Board?
5. Has the company engaged with their assurance provider?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask (continued)

ESG considerations:

1. What are the company's material environmental and social opportunities and risks? This will include consideration of impacts of areas such as environment, waste, biodiversity, water, health and safety of employees and the community, community engagement and investment, human rights and employee diversity and inclusion, and the overall governance of each of these areas.
2. Does the board have visibility of the company's strategy in relation to these material environmental and social opportunities and risks?
3. Is there a governance framework in place for managing social and environmental issues? Does responsibility lie with a 'C-class' executive?
4. How does the company meet its obligations to investors to disclose on material environmental and social sustainability risks?
5. Does the company report publicly on environmental and social strategy, performance, governance and risks? Has the board ever read the report?
6. Does senior management report to the board on environmental and social issues? Are environmental and social targets aligned to broader business objectives?
7. If environmental and social data is reported externally, are these areas managed internally or is the external reporting just for show? Could the company be accused of 'greenwashing' in its external disclosures?
8. Is the company exposed to material environmental and social risks in its supply chain? How are risks in the supply chain identified and managed?
9. Which committee is responsible for oversight of social and environmental issues and their reporting? Is the board aware of its role and responsibilities in relation to these issues? Does it have sufficient knowledge to be able to challenge senior management?
10. Is the board aware of the true value of the company's operations: that is, when considering economic, social and environmental externalities, does the company make a positive or negative contribution? Does the organisational strategy consider these impacts?
11. Has the board performed a self-assessment so as to determine whether governance practices are aligned with what stakeholders may expect?
12. How does the board's composition need to adapt to be better positioned to respond to ESG?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

Australian Sustainability Reporting Standards (ASRS) framework

- The directors have not been briefed on the company's progress and action plan to meet the requirements of ASRS.
- There is a lack of management accountability over the implementation of the ASRS requirements.
- The sustainability team spend most of their effort collecting data, but little action is taken.
- Climate-related data and information is not reliable, or not regularly collated or available.
- The board does not have oversight of the company's climate strategy and/or related performance reporting (internal or external).

ESG considerations

- An absence of environmental or social considerations in the overall strategic company objectives.
- Environmental and social issues and costs are rarely reported, discussed or considered at board level, or publicly disclosed as part of the company reporting process.

- No executive is accountable for environmental and social issues.
- Social or environmental sensitivities impact corporate operations or share price.
- Social or environmental incidents occur with little warning.
- The organisation struggles to answer questions from investors and analysts which extend beyond corporate financial performance.
- ESG is mentioned to please external stakeholders but there is no structured plan on how to achieve objectives and implement the changes needed.
- The company is working in an issues-rich space that has attracted the attention of activists.
- There is a lack of company knowledge of who the online advocates, activists and regular commentators about the company and its interests are, what their arguments are, and how influential and connected they are.
- There is an awareness that dedicated influencers are reaching influential actors, like politicians, regulators, shareholders and staff with criticisms of the company.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

THE AUSTRALIAN SUSTAINABILITY REPORTING STANDARDS (ASRS)

The Australian Sustainability Reporting Standards (ASRS) represent a significant step in embedding sustainability, in particular, climate-related financial disclosures into corporate reporting in Australia. These disclosures are governed by two standards issued by the Australian Accounting Standards Board (AASB): AASB S1,¹ a voluntary standard for general sustainability-related financial information, and AASB S2,² a mandatory standard focused specifically on climate-related disclosures. Both standards are closely aligned with international equivalents, IFRS S1 and IFRS S2, with minimal variations to suit the Australian context.

Mandatory sustainability reporting in Australia was enacted through the *Treasury Laws Amendment (Financial Market Infrastructure and Other Measures) Act 2024* (the Act), which mandates that certain entities disclose their climate-related plans, financial risks, and opportunities in accordance with AASB S2. This Act passed amendments to Corporations Act. Accordingly, ASIC is the regulator for the mandatory sustainability reporting regime in Australia.

The focus of this chapter is on the mandatory sustainability reporting regime and the mandatory standard: AASB S2 Climate-related disclosures.

For further information, refer to KPMG's *Australian Sustainability Reporting legislation and standards Guide*.

Reporting entities in scope

The regulatory framework mandates sustainability reporting for entities that are required to lodge financial reports under Chapter 2M of the Corporations Act and meet specific thresholds related to their emissions reported under the *National Greenhouse and Energy Reporting Act 2007* or revenue, assets, or employee numbers. The financial-related thresholds of revenue and assets are defined with reference to existing Australian accounting standards.

The regulatory framework is being implemented in a phased approach depending on the reporting entity's emissions or size. Group 1 entities, the largest, begin reporting from 1 January 2025, followed by Groups 2 and 3 in subsequent years. The climate-related disclosures are to be included in a sustainability report that forms part of the entity's annual reporting suite and must be lodged with the Australian Securities and Investments Commission (ASIC) in line with existing annual financial reporting timelines. The table below provides a visual representation of the three-phased approach to the implementation of mandatory sustainability reporting in Australia.

	Entities required to report under Chapter 2M			
	Meet two of three thresholds:			National Greenhouse and Energy Reporting (NGER) Reporters
	Gross assets	Revenue	Employees	
Group 1 First annual reporting periods beginning on or after 1 January 2025	\$1 billion or more	\$500 million or more	> 500	Above NGER publication threshold
Group 2 First annual reporting periods beginning on or after 1 July 2026	\$500 million or more	\$200 million or more	> 250	All other NGER reporters
Group 3 First annual reporting periods beginning on or after 1 July 2027	\$25 million or more	\$50 million or more	> 100	N/A

¹ <https://standards.aasb.gov.au/aasb-s1-sep-2024>

² <https://standards.aasb.gov.au/aasb-s2-sep-2024>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Australian boards and executives are currently focused on establishing robust governance structures, ensuring data accuracy, and upskilling internal teams to meet the new reporting obligations. This includes defining materiality processes, clarifying accountability, and preparing for external assurance.

As a director of a reporting entity, your role in sustainability reporting is both important and manageable with the right systems and awareness in place. You are expected to exercise care and diligence to act as a reasonable person would in your position, when overseeing the preparation of your organisation's sustainability report. This means understanding your legal obligations under the Corporations Act and the Australian Sustainability Reporting Standards (ASRS), particularly AASB S2, and ensuring that your organisation has the right processes to identify, assess, and monitor climate-related financial risks and opportunities.

While you can rely on experts and advisers to help with technical aspects, it's important that you make your own informed judgement

about the advice you receive. You're not expected to be a climate scientist or data analyst, but you are expected to understand the implications of climate-related risks for your organisation and to ensure that the report reflects those risks appropriately. Your oversight helps ensure that the sustainability report is a reliable source of information for investors, regulators, and other stakeholders.

Assurance requirements

Assurance requirements will be phased in over time, with increasing levels of scrutiny and rigour expected from entities as their capabilities mature. In January 2025, the Auditing and Assurance Standards Board (AUASB) approved its final sustainability assurance standards and established an assurance phasing model. This commences with mandatory limited assurance over some AASB S2 areas, and builds up to reasonable assurance over all AASB S2 disclosure areas by FY29 for Group 1 entities, FY30 for Group 2 entities and FY31 for Group 3 entities.

AUASB phased assurance timeline

Extract: ASSA 5010 Timeline for Audits and Reviews of Information in the Sustainability Reports under the Corporations Act 2001

Year commencing	Year 1 ¹	Year 2	Year 3	Year 4 ²	Year 5	Year 6
Group 1	1/1/25 to 30/6/26	1/7/26 to 30/6/27	1/7/27 to 30/6/28	1/7/28 to 30/6/29	1/7/29 to 30/6/30	1/7/30 to 30/6/31
Group 2	1/7/26 to 30/6/27	1/7/27 to 30/6/28	1/7/28 to 30/6/29	1/7/29 to 30/6/30	1/7/30 to 30/6/31	1/7/31 to 30/6/32
Group 3	1/7/27 to 30/6/28	1/7/28 to 30/6/29	1/7/29 to 30/6/30	1/7/30 to 30/6/31	1/7/31 to 30/6/32	1/7/32 to 30/6/33
Governance	Limited	Limited	Limited	Reasonable	Reasonable	Reasonable
Strategy – Risks and opportunities ³	Limited ⁴	Limited	Limited	Reasonable	Reasonable	Reasonable
Climate resilience assessments/scenario analysis	None ⁵	Limited	Limited	Reasonable	Reasonable	Reasonable
Transition plans	None ⁵	Limited	Limited	Reasonable	Reasonable	Reasonable
Risk management	None ⁵	Limited	Limited	Reasonable	Reasonable	Reasonable
Scope 1 and 2 emissions	Limited	Limited	Limited	Reasonable	Reasonable	Reasonable
Scope 3 emissions	N/A ⁵	Limited	Limited	Reasonable	Reasonable	Reasonable
Climate-related Metrics and Targets	None ⁵	Limited	Limited	Reasonable	Reasonable	Reasonable

¹ Group 1 entities with years commencing 1 January to 30 June will be subject to the Year 1 provisions twice (e.g. years commencing 1/1/25 and 1/1/26). Reporting of Scope 3 emissions is required for years commencing 1/1/26 to 30/6/26 for these Group 1 entities.

² Group 3 is to be subject to reasonable assurance across all disclosures by years commencing 1 July 2030.

³ The phasing for assurance on statements that there are no material climate-related risks and opportunities would be the same as for 'Strategy – Risks and Opportunities'.

⁴ Only subparagraphs 9(a), 10(a) and 10(b) of AASB S2 Climate-related Disclosures.

⁵ 'N/A' means disclosure is not required while 'None' means disclosure is required but not subject to assurance.

⁶ Refer to Are you ready for ISSA 5000? – a KPMG guide for understanding and preparing for the new sustainability assurance standard.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Liability framework

Climate-related financial disclosures will be subject to the current legal framework in various areas including directors' duties, misleading representation provisions and reporting requirements. These requirements are embedded in the *Corporations Act 2001*, *Australian Securities and Investment Commission Act 2001* and the *Competition and Consumer Act 2010*.

Directors are expected to oversee the integrity of disclosures and ensure appropriate governance systems are in place to manage climate-related risks. The Directors' Declaration is a fundamental component of the Sustainability Report and must be formally approved and signed by the board of directors. This declaration affirms that the climate-related disclosures, such as the climate statements and any accompanying notes, are prepared in accordance with AASB S2 and the *Corporations Act 2001*.

The Act introduces a modified liability framework during the first three-year transition period (financial years commencing between 1 January 2025 and 31 December 2027), limiting legal exposure for disclosures related to Scope 3 emissions, scenario analysis, and forward-looking statements. Legal action is restricted to criminal law or instigated by ASIC. The modified liability is also extended to cover all forward-looking statements relating to climate for the first financial year for Group 1 entities. This framework aims to encourage transparency while acknowledging the complexity and evolving nature of climate-related reporting. During the initial three-year transitional period (covering financial years commencing between 1 January 2025 and 31 December 2027) the directors' declaration is also modified. This means that directors are required to declare that they have taken 'reasonable steps' to ensure the report complies with the relevant requirements. From financial years beginning 1 January 2028 onwards, this declaration becomes unqualified, requiring directors to attest that the report is fully compliant.

At the time of publication, there are proposed legislative changes to extend the liability framework to apply to voluntary sustainability reporting too.

ASIC REGULATORY GUIDE 280: SUSTAINABILITY REPORTING³

To support a smooth transition, ASIC will adopt a proportionate and pragmatic approach to enforcement in the early years of implementation. [Regulatory Guide 280: Sustainability Reporting](#) (RG 280), issued by ASIC in March 2025, offers detailed guidance on the implementation of the ASRS. The guide outlines the legal framework, reporting obligations, and ASIC's expectations for compliance, aiming to support consistent, high-quality climate-related financial disclosures aligned with AASB S2.

The Guide provides guidance on areas including:

- Clarification of directors' duties: directors are expected to exercise oversight, ensure robust internal systems, and critically review sustainability disclosures. This aligns with their duty of care and diligence.
- Modified liability settings: protected statements in the legally required Operating and Financial Review (OFR) are covered under a modified liability regime. However, disclosures outside the sustainability or auditor's report are only protected if they are exact reproductions. Voluntary disclosures, such as those in investor presentations or AGM responses, are not protected.
- Expanded guidance on scenario analysis and Scope 3 emissions: entities must use at least two climate scenarios in their analysis – one reflecting a 1.5°C scenario and another reflecting a temperature rise above 2.5°C. Practical guidance is also provided for estimating and measuring Scope 3 emissions, acknowledging the challenges involved.
- ASIC's enforcement approach: ASIC will adopt a proportionate and pragmatic approach during the transition phase. It will conduct annual surveillance of sustainability reports and publish findings to promote best practices.

3 [rg280-published-31-march-2025.pdf](#)

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

2. ESG considerations: questions that company directors should ask

It has become more common for independent bodies (for example, the Australian Council of Superannuation Investors (ACSI)) to publish sustainability indices and reports that discuss commonly used sustainability frameworks aimed at improving the quality of sustainability-related information provided by companies. These reports provide a number of benchmarks against which investors can comparatively assess company performance and are driving an approach to standardise sustainability disclosures.

There is now much more of a regulatory onus on companies and their directors to take responsibility for sustainability-related risks, opportunities, and the potential impact on company performance.

The ASX Principles (4th edition), also recognises that a company's operations impact on a wide range of stakeholders and that an entity should be aware of the increasing calls globally for the business community to address the effects of environmental and social responsibility. Recommendation 7.4 indicates that a listed entity should disclose whether it has had any 'material exposure' to economic, environment and social sustainability risks, and to discuss how it intends to manage those risks. The definition of 'material exposure' recognises that ESG risks are inherently linked with economic and/or financial risk.

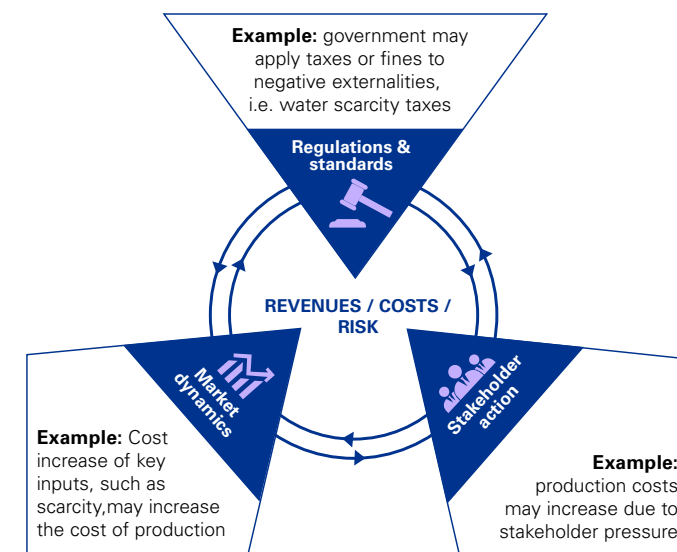
KEY CONCEPTS

Institutional investors and analysts are today commonly applying ESG factors in their assessments of the long-term performance of companies. Integrating ESG into the investment decision is to approach investing without sacrificing risk-adjusted return and creating value while also improving the long-term return.

The Australian Sustainable Finance Taxonomy Roadmap establishes a standardised classification system for defining 'green' or 'transition' economic activities. This taxonomy aims to provide clarity and

consistency in identifying sustainable economic activities, which is essential for the development of sustainable finance products, accurate data collection, and fair comparisons of sustainability performance across financial institutions. This initiative fits into the broader Sustainable Finance Roadmap of the Australian Government by supporting the nation's transition to a low-carbon economy.

Drivers



The key drivers of the enhanced focus on ESG are the increasing power of stakeholders, changing market dynamics and the emergence of regulations and standards. These are collectively referred to as the 'drivers of internalisation', as any one of these factors can result in an external impact on the organisation by changing to one which directly affects the operation and profitability of the company. For example, 'green buildings' were once seen as niche, but have now become mainstream, due to market demand for these type of buildings.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The pressure to transparently demonstrate how ESG assessment criteria are utilised across governance, processes and reporting is largely due to stakeholder demands to understand more about the sustainability of a company and its key decisions. Investors and analysts are the stakeholders with the most direct impact on companies, but the indirect impacts are forever strengthening.

The power of stakeholders has grown exponentially with the rise of social media and the knowledge is shared globally almost instantly.

Much of the value of companies today is inherent in intangible assets, such as brand names and reputation, rather than traditional tangible assets. These intangible assets are closely linked to ESG factors and their value can be readily destroyed if these factors are not managed.

There are also a growing number of regulatory requirements driving the increased focus on ESG issues, such as the Financial Services Council (Standard 20), the ASX Principles and the signatory requirements under the United Nations (UN) Principles for Responsible Investment (PRI). Regulatory requirements in other jurisdictions are also increasingly driving shareholder expectation of reporting in Australia.

Much of the current focus for investors and regulatory bodies is on responding to climate change. This is the case for Australia and the ASRS where the regulation has adopted a climate-first approach.



Case study: Volvo Group – the True Value of Volvo's electric buses

Volvo Group wanted to show leadership in the transport sector and the global sustainable development movement by quantifying the environmental and social value created by their electric buses. To do this, they calculated (using KPMG's True Value methodology), a true Total Cost of Ownership (TrueTCO), which took into account not only the financial costs and returns associated with building and operating electric buses, but also the environmental and social costs and returns.

For example, cost of ownership calculations traditionally only focus on direct acquisition and operating costs, such as vehicle leases, fuel, driver salaries, garage and maintenance costs. However, there are other, indirect/non-financial costs (and benefits) that are associated with electric vehicles, including:

- negative effects of noise and pollution on public health
- environmental impacts of manufacturing the fuel
- contributions to climate change.

Using proxies and measures such as greenhouse gas emissions comparisons (including carbon prices/taxes), noise and air pollution levels associated with electric versus diesel engines, fuel/energy consumption data and a value of time per hour per passenger (based on government economic estimates), a true cost of ownership was calculated. The results indicated that the TrueTCO of an electric bus is lower than that of a diesel bus, by a significant amount.

The findings transformed the business case for electric buses. Using traditional accounting techniques, electric buses looked like a high-cost, low-return investment. However, when incorporating social and environmental costs and benefits, it was determined that Sweden could save up to approximately US\$225 million per year, of which US\$45 million could be savings in public healthcare costs. In addition, passengers could save 14 million hours of travel time per year and Sweden's carbon emissions could be reduced by 84,000 tons per year (approximately equivalent to the annual per capita emission of 15,000 Swedish citizens).

The benefits for Volvo? The analysis has helped Volvo to position itself as a leader in sustainability and the development of sustainable cities, enhancing its brand reputation and an opportunity to leverage this with government and key stakeholders, thereby managing multiple risks and creating new opportunities.

'The results of this analysis have the potential to change perceptions, influence decision-makers and ultimately to transform urban environments worldwide.'

Niklas Gustavsson, Chief Sustainability Officer, Volvo Group

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

STRATEGY

A comprehensive ESG strategic framework is part of the overall company strategic framework. Decisions as to the extent of the internalisation of externalities across the value chain should be taken at senior levels within an organisation, applying a risk management approach to minimising potential future costs and promoting the long-term sustainability of the organisation. At face value, ESG risks are largely non-financial, however, financial markets are increasingly costing in the value of ESG risks in investment decisions. Further, social and environmental issues inevitably result in economic impacts; it's just a matter of timing.

The key to understanding non-financial risks is to understand the integration and impact of these risks on the economic success or failure of an organisation, including:

- regulatory risk due to complex changes to the regulatory landscape
- reputational risk and damage to corporate reputation and value through adverse publicity
- competitive risk from fast-changing market dynamics, uncertainty of supply, and price volatility of key inputs
- exposure to legal action through, for example, non-disclosure of environmental, social and governance information.

Oversight of the effective management of non-financial risks and opportunities is the responsibility of the board, and an increasing number of stock exchanges and governments are seeking more public disclosure on ESG governance in recognition of this responsibility. A board should consider the relationship between non-financial and financial risks, and whether these are adequately identified and addressed by the company.

Effective oversight of an ESG framework also requires consideration and challenge on the extent of ESG integration into corporate strategic planning, both in the short and long term. The board should ensure the ESG issues identified as most material to the organisation are connected to existing strategy and risk management processes.

IDENTIFYING MATERIAL RISKS

Effective ESG risk management requires a robust mechanism for the identification and assessment of issues that are material to the organisation. Materiality with respect to ESG risks does, however, involve a more qualitative assessment of issues than is traditionally applied in financial reporting. The ASX Principles define material exposure as 'a real possibility that the risk in question could substantively impact the listed entity's ability to create or preserve value for security holders over the short, medium or long term.'⁴

Guidelines such as the Association of British Insurers on Responsible Investment in the UK recommend a regular review of ESG risks by the board of directors.

Directors should enquire of management whether a robust materiality assessment process and ESG risk assessment are in place, and how key non-financial and financial risks interact across their business. This includes understanding where the key non-financial exposures are across the organisation's value chain and the potential subsequent cost/impact, such as costs arising from the impact of extreme weather events and reputational damage associated with human rights issues/claims. This assessment may also identify economic opportunities across the environmental and social impacts observed.

Identifying and understanding the material ESG issues, and the risks and opportunities they represent, is a critical part of promoting the long-term sustainability of the organisation. The board should enquire of management whether there is strong alignment between the materiality assessment process for ESG issues and the organisation's existing risk management and strategy development processes.

4 ASX Corporate Governance Principles, 4th edition, 2019, recommendation 7.4

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

KPIs AND TARGETS

An effective way for directors to assess progress against identified material risks is to ensure management implement targets and KPIs associated with each material indicator. It is the responsibility of directors to ensure that management has implemented systems, procedures and controls to gather reliable and timely information about key environmental and social trends and issues.

Directors should understand and agree on management's selection of key performance indicators regarding environmental and social performance, and ensure periodic reviews take place of company and individual performance against these indicators. The board and management should engage in discussions over the types of performance indicators that need to be set, measured, rewarded and communicated. The indicators selected for assessment should be based on appropriate data collection and reporting systems, and, most importantly, should be relevant to the company's material ESG issues identified through its materiality assessment.

It is currently popular for companies to publish ESG targets, particularly in relation to climate change (e.g. setting targets to achieve net zero by 2050). But care should also be taken to ensure these targets are achievable and supported by real action. In 2021, a shareholder activist group took Santos to court to argue that it did not have a sufficiently clear and credible plan to support its plans to reach net zero emissions by 2040.⁵ There has been no outcome to the court case yet, but investors and analysts are becoming increasingly savvy and companies should ensure that their targets and external disclosures are achievable and realistic to avoid claims of greenwashing.

⁵ Refer to The Guardian, 2021, Santos sued for 'clean fuel' claims and net zero by 2040 target despite plans for fossil fuel expansion, <https://www.theguardian.com/australia-news/2021/aug/26/santos-sued-for-clean-fuel-claims-and-net-zero-by-2040-target-despite-plans-for-fossil-fuel-expansion>

GLOBAL SUSTAINABILITY REPORTING

Sustainability reporting is now standard among nearly all of the world's largest 250 companies and most top 100 firms in each jurisdiction. There's been a notable rise in carbon reduction target disclosures and a growing, though still limited, focus on biodiversity. Many companies are acting ahead of regulatory deadlines to better inform stakeholders and prepare for compliance. 96% of G250 companies report on sustainability, including all of the top companies in Japan, Malaysia, Singapore, South Africa, South Korea, and Thailand. Furthermore, setting carbon targets has become part of business as usual with 95% of G250 companies publishing carbon targets, representing a 15% increase since 2022.

This increase in voluntary reporting is now supported by incoming frameworks, with the CSRD making reporting on ESG and sustainability mandatory for around 50,000 companies, including thousands headquartered outside of the EU. Some companies are already moving towards compliance with ESRS and nearly half of European companies have adapted the EU taxonomy. GRI standards remain the most popular guidelines and standards with 77% of G250 companies adopting. The use of GRI has remained stable whilst the use of the SASB standards, which have since been superseded by the ISSB, rose from 49% in 2022 to 56% in 2024 within G250 companies.

The global landscape for sustainability reporting is undergoing rapid transformation, driven by increasing regulatory expectations and stakeholder demand for transparency on climate-related risks and opportunities. Internationally, jurisdictions such as the European Union, Asia and Canada are advancing climate disclosure regimes. The International Sustainability Standards Board (ISSB) has played a pivotal role in shaping global standards, with many countries either adopting or aligning with its frameworks. The ISSB was officially established in November 2021 by the IFRS Foundation. The ISSB's first climate-related disclosure standard, IFRS S2, came into effect in January 2024, marking a significant step in global sustainability reporting. The ISSB incorporates the former Task Force on Climate-related Financial Disclosure (TCFD) principles and expands them into a broader, standardised framework for sustainability reporting.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The [AASB Staff Paper June 2025](#) included a useful horizon analysis of different judgements' adoption of the ISSB standards.

Australia had adopted IFRS S1 and IFRS S2, with minimal amendments for the Australian context, with the formalisation of the ASRS in September 2024. The focus is on balancing investor demand for sustainability information with the time required for companies to prepare, upskill, and establish necessary systems. Larger listed companies and financial institutions are expected to lead the implementation, with transitional periods likely to allow for readiness. The standards aim to enhance transparency and comparability in sustainability reporting, aligning Australian entities with global practices.

The release of the ASRS is driving a different perspective and set of conversations in boardrooms, causing business leaders to stretch their thinking and ensure that from the top down they are making strategic decisions that take climate and broader ESG considerations more into account. As of December 2024, 97% of Australia's top companies continue to provide sustainability reporting, which marginally outperforms 2024 performance of global peers.⁶ Further to this, 90% of ASX 100 companies recognise climate as a financial risk, with 76% reporting in line with the recommendations of the Task Force on Climate-Related Financial Disclosures, putting these entities in a good position to report against the Australian Sustainability Reporting Standard (ASRS).

The Corporate Sustainability Reporting Directive (CSRD) is a European Union initiative that mandates sustainability reporting for a broader range of companies than its predecessor, the Non-Financial Reporting Directive (NFRD). The CSRD requires companies to report on ESG factors using the European Sustainability Reporting Standards (ESRS). It applies to large EU companies, listed SMEs, and non-EU companies with significant EU operations, with phased implementation starting in 2024 for large companies.

The EU commission has since published its first 'Omnibus' package, responding to calls for simpler and more streamlined sustainability reporting requirements. The omnibus puts forward several proposals which would make significant changes to the scope, timing and content of the Corporate Sustainability Reporting Directive (CSRD), Corporate Sustainability Due Diligence Directive (CSDDD), EU Taxonomy, and carbon border adjustment mechanism (CBAM).⁷

The Canadian Sustainability Standards Board (CSSB) has released its first two Canadian Sustainability Disclosure Standards (CSDS) to support companies in identifying and reporting sustainability information. The standards are aligned with the ISSB baseline standards IFRS S1 and IFRS S2 with specific modifications for the Canadian context. The CSSB Standards are set to be effective for annual reporting periods on or after 1 January 2025 and reporting remains on a voluntary basis.⁸

Within the Asia-Pacific region, sustainability-related disclosures are expanding beyond environment to encompass other topics such as social impact and considerations of the broader value chain. In China, the Ministry of Finance issued an exposure draft of Corporate Sustainability Disclosure Standards in 2024 which is largely aligned with IFRS S2, representing a first step towards establishing a comprehensive sustainability reporting framework for companies in China. Similarly, both Japan and Malaysia are building reporting frameworks in alignment with the ISSB reporting standards.

⁷ Refer to KPMG Netherlands, ESG Regulatory Essentials, [ESG Regulatory Essentials: March 2025 – Issue 16](#)

⁸ Refer to KPMG Canada, CSSB Sustainability Reporting, [CSSB | Sustainability reporting – KPMG Canada](#)

⁶ [australian-sustainability-reporting-trends-november-2024.pdf \(SECURED\)](#)

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

GOVERNANCE AND CULTURE

Effective management of non-financial risks and opportunities requires a robust governance structure. The ESG framework should detail the governance arrangements in place to oversee the effective identification and management of ESG risks across the business, setting the tone at the top for the rest of the organisation.

While the board is ultimately responsible for the oversight of non-financial risk, this is more commonly undertaken by an executive or committee of the board responsible for the oversight of ESG matters. Regardless of the approach, clear reporting lines and responsibilities should be established and communicated. Some companies are choosing to set up a specialised committee to oversee non-financial matters.⁹

It is the responsibility of directors to ensure they receive adequate and appropriate training and continuous development in order to ensure they are fully equipped to carry out their roles, make informed decisions and adequately challenge management in the area of ESG risk management. The ASX Principles recommend that a listed entity has a program in place to provide appropriate training and professional development opportunities for directors so they are able to maintain the skills and knowledge to perform effectively in their roles.¹⁰ Having at least one board member with a demonstrated sustainability background or experience is now becoming one of the criteria that analysts are using in scoring company ESG performance for sustainability indices such as Bloomberg ESG.

Boards are increasingly expected to promote and support a corporate culture which embeds the consideration of environmental and social issues into decision-making and performance throughout the organisation. The ESG governance framework should include clear expectations of how risk and opportunities are managed and who within the organisation is accountable. Raising the visibility and importance of the issues through specific KPIs for senior management that cascade down the organisation, is one way the board can set the tone and influence corporate culture

⁹ See Chapter 3.3 Board Committees

¹⁰ ASX Corporate Governance Principles, 4th edition, 2019, recommendation 2.6

ROLE OF THE BOARD

Ultimately the board is the G in ESG and plays a key role in leading a company's commitment to ESG issues and their consideration and integration across the organisation. This can be done by:

- recognising responsibility for ESG issues at board level and ensuring that ESG governance is appropriately delegated across the organisation
- providing clear strategic direction on ESG issues for the short and long term in order to allow for the development of a more detailed ESG framework
- monitoring the assessment and regular review of material issues
- oversight and challenge of management's financial and non-financial assessment of material risks
- challenging the performance of the company in relation to ESG targets and related KPIs
- establishing a corporate culture that supports the effective management of ESG-related issues, in recognition of their importance to the long-term sustainability of the organisation
- oversight of the depth and breadth of ESG-related reporting and the alignment with recognised frameworks and initiatives
- requiring senior management approval and external assurance over ESG reporting in order to ensure confidence in the information and the business systems and processes from which it is sourced
- undertaking training to keep up to date with the evolving issue of ESG and to be able to lead and challenge management.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- Sustainability reporting survey: Global and Australian Insights <https://kpmg.com/au/en/insights/economics-geopolitics/sustainability-reporting-survey-2024.html>
- AASB June 2025 Staff Paper which includes a reporting horizon scan that summaries domestic and international sustainability reporting updates https://aasb.gov.au/media/quihjmtg/08-1_sp_sr_horizon_scanning_m213_pp.pdf
- ASIC Regulatory Guide 280 Sustainability reporting – KPMG Australia <https://kpmg.com/au/en/insights/financial-reporting/sustainability-climate-change/asic-rg280-sustainability-reporting.html>
- Australian sustainability reporting standards finalised – KPMG Australia <https://kpmg.com/au/en/insights/financial-reporting/sustainability-climate-change/australian-sustainability-reporting-standards-legislation-finalised.html>
- Prepare for global and Australian sustainability standards – KPMG Australia <https://kpmg.com/au/en/insights/financial-reporting/sustainability-climate-change/issb-sustainability-reporting-disclosures-guide.html>
- [rg280-published-31-march-2025.pdf](#)
- <https://standards.aasb.gov.au/aasb-s1-sep-2024>
- <https://standards.aasb.gov.au/aasb-s2-sep-2024>
- ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019
- KPMG, KPMG Sustainability Services <https://home.kpmg/au/en/home/services/advisory/risk-consulting/climate-change-sustainability-services/sustainability.html> KPMG, KPMG Survey of Corporate Responsibility Reporting 2020 <https://home.kpmg/xx/en/home/insights/2020/11/the-time-has-come-survey-of-sustainability-reporting.html>
- United Nations, Sustainable Development Goals, <https://sdgs.un.org/goals>

- Global Reporting Initiative, <https://www.globalreporting.org/standards/>
- ASIC publishes final sustainability reporting guidance for companies <https://www.aicd.com.au/risk-management/framework/climate/asic-publishes-final-sustainability-reporting-guidance-for-companies.html>

For further information please contact:



Adrian King
Partner in Charge,
Climate Change & Sustainability
Services, KPMG Australia
avking@kpmg.com.au



Julia Bilyanska
Partner in Charge,
Climate Change & Sustainability
Services, KPMG Australia
jbilyanska@kpmg.com.au



Sarah Newman
Partner,
Climate Change & Sustainability
Services, KPMG Australia
senewman@kpmg.com.au

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

19. Safeguarding of Vulnerable People

The safeguarding of vulnerable people refers to the steps an organisation takes to ensure their operations, investments and business decisions do not harm the customers, consumers, or communities they serve. This includes providing safety, care and support to those who may be at greater risk of exploitation due to the organisation's operations. Safeguarding is tactical. Safeguarding goes beyond theory to embed actual measures, or safeguards, to keep vulnerable people safe.

The safeguarding of vulnerable people in this chapter refers to an organisation's customers and consumers. It challenges organisations to look beyond their internal sphere of influence and take an outward-looking view on their impact in relation to vulnerable people across their customer and consumer network, operations and environment.

In this chapter

- Why does the safeguarding of vulnerable people matter?
- The definition of a vulnerable person
- Key concepts and the emergence of 'safeguarding culture'
- Legislation, compliance, and drivers
- Vulnerable people governance framework
- Risk and measures of success
- The role of the board – reporting and confidence

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Does the board have oversight on where interactions with vulnerable people may occur across the organisation, including across the consumer/customer journey?
2. What specific measures, policies and frameworks have been put in place to identify and protect vulnerable groups that the organisation impacts?
3. Does the board have visibility of the organisation's safeguarding strategy, reports, governance framework, and measures of success?
4. Who is specifically responsible for overseeing initiatives to support vulnerable consumers or customers, and how does the board empower them to make necessary changes?
5. In what ways does the organisation engage with vulnerable people to understand their unique needs and to ensure that services are accessible, inclusive and beneficial to them?
6. What training and resources are provided to employees to recognise and respond to the needs of vulnerable consumers or customers?
7. How does the board hold management accountable for ensuring the safeguarding strategy and its policies are implemented and meet the board's expectations?
8. How are incidents of harm or abuse reported, monitored, and resolved within the organisation?
9. How quick and effective are our response mechanisms? Are they proactive or reactive?
10. Has the board established KPIs or KRIs for identifying and managing risks to the organisation's vulnerable consumers or customers?
11. What is the process for conducting due diligence to prevent exploitation or harm to vulnerable people that may be caused indirectly by our business operations?
12. What is the procedure for regularly reviewing and updating the safeguarding strategies to adapt to new threats or changes in the community?
13. What are the potential risks or challenges faced in implementing effective safeguarding practices, and how is the board addressing them?
14. How is the organisation integrating the safeguarding of vulnerable people into all business functions and activities, including customer service and experience, HR, and operations?
15. Does the board have the appropriate skills mix to consider and account for their vulnerable customers, consumers and communities?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- Board members and senior management don't understand where their organisation interacts with, and impacts vulnerable people, what safeguarding measures are, who they impact and why they're important.
- There is no safeguarding strategy, policies, plan, or frameworks.
- No executive in the organisation is held accountable for any issues related to the governance of vulnerable consumers and customers.
- There are no safeguarding-related measures included in the organisation's objectives or targets.
- Board members, employees and volunteers have received insufficient training on recognising and responding to vulnerable consumers and customers.
- There is an unwillingness to update or revise policies and procedures in response to feedback, incidents, or changes in best practices.
- There is no consideration of the suitability and safety of employees, volunteers or contractors to serve and support vulnerable consumers and customers the organisation interacts with.
- There is no consideration of vulnerability across the consumer or customer journey.
- Safeguarding risks are not considered or inadequately assessed throughout the organisation's services and operations.
- There is no regular process of risk monitoring to protect vulnerable people including within the organisation, its services, in its supply chain or partners.
- The protection and wellbeing of vulnerable people is mentioned to please external stakeholders but there is no structured plan on how to achieve objectives and implement the changes needed.
- There are repeated violations of legal or regulatory requirements related to vulnerable or marginalised groups.
- The organisation's operations enable harmful or predatory behaviour, including abuse or commercial gain from adverse sales, claims and overcharging.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

WHY DOES THE SAFEGUARDING OF VULNERABLE PEOPLE MATTER?

Safeguarding an organisation's vulnerable people is a legal, ethical and social obligation. Failure to manage the risk that an organisation adversely impacts vulnerable people it serves and supports can lead to brand and reputational damage, potential claims, financial loss and be detrimental to a person's life.

Across Australia, 28.5 percent of children have experienced sexual abuse.¹ This statistic doesn't include harm caused upon other vulnerable groups, such as older people, people living with disability or those experiencing family domestic violence. Organisations must evolve to protect their people, understand their impact, and improve these historically devastating figures.

The safeguarding of vulnerable people is a critical component of responsible and ethical business practices, with a focus on the 'S' (social) pillar of ESG. Being known as a socially responsible company that safeguards the vulnerable people it impacts, enhances its long-term resilience, its ability to respond to regulatory compliance pressures and strengthens its relationships and trust with employees, government, regulators, and the broader community.

Royal Commissions, inquiries and recent events including natural disasters and the global pandemic have all drawn increasing attention to the risks and vulnerability of customers, across all sectors. These inquiries highlighted that many vulnerable populations have historically been failed by organisations who don't have sufficient and robust safeguarding measures in place.

Organisations have a role, and extensive positive obligations, in preventing harm and protecting vulnerable people from harm.

¹ The Australian Child Maltreatment Study (ACMS), The prevalence and impact of child maltreatment in Australia: Findings from the Australian Child Maltreatment Study: 2023 Brief Report, <https://www.acms.au/resources/the-prevalence-and-impact-of-child-maltreatment-in-australia-findings-from-the-australian-child-maltreatment-study-2023-brief-report/>

THE DEFINITION OF A VULNERABLE PERSON

Every organisation, no matter their services or sector, will interact with vulnerable people. This may vary depending on the nature, environment and operations of the organisation, program or activity. The ability to recognise a vulnerable person in different situations is crucial to be able to effectively prevent and protect from harm and keep people safe.

The main types of vulnerability can include:

- 1. Personal** – vulnerabilities based on personal characteristics including age, people living with disability, mental illness, learning difficulties or low levels of literacy, people from culturally or linguistically diverse backgrounds or sexual preferences.
- 2. Situational** – vulnerabilities due to their situation, including people experiencing financial stress, domestic violence, homelessness or people marginalised due to unequal power relationships in society.
- 3. Place** – vulnerabilities due to the place or location including those from low socio-economic, isolated or remote communities, including Indigenous communities or those in areas prone to conflict, high levels of crime, natural disasters or weather events.

Vulnerability can be permanent, incidental, or temporary; it can also vary and intersect.

Examples of interactions with vulnerable people:

- **An entertainment company holds an event** where accessibility, inclusion and child safety requirements must be considered and accounted for.
- **Where sporting coaches or education providers** have direct contact with children, families and communities and hold an inherent power imbalance.
- **Core services or programs** such as banks, energy, or telecommunications service providers where vulnerable customers are not exploited, are given information to make informed decisions and are provided with products and services that are accessible and inclusive.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

It's essential for organisations to understand the nature of their interactions with vulnerable people to ensure their operations don't cause harm, abuse or exploitation, enable harmful or predatory behaviour, and that they are providing appropriate and effective support to their consumer groups.

KEY CONCEPTS AND THE EMERGENCE OF 'SAFEGUARDING CULTURE'

The emergence of safeguarding as a business risk is multifaceted. It reflects a broader societal shift towards greater accountability and transparency, fuelled by social movements and public scrutiny. It also acknowledges the deep interconnectedness of customers and ever-evolving operating models. It recognises that harm can occur at any point, often beyond direct control but within the sphere of the organisation's influence. With the emergence of the ESG social pillar, the importance of protecting an organisation's customer, consumers and communities has never been more prevalent.

Understanding and addressing safeguarding risk is no longer optional but a critical component of corporate responsibility. As global awareness rises and regulatory frameworks become increasingly more stringent, organisations must ensure they are not only compliant with relevant legislation, regulation and guidelines, but are also actively fostering safe environments and taking thorough ethical preventative actions where required.

'Safeguarding culture' refers to how an organisation ties safeguarding into every aspect of its operations and services. A robust and effective safeguarding culture is centred on the welfare and protection of all vulnerable customers or consumers whilst also creating conditions for them to thrive.

Some key concepts when developing your safeguarding strategies, culture and assessments include:

- 1. Legislation** – organisations operating in Australia must navigate legislation designed to protect the rights of vulnerable people. These are explored in more detail later in this chapter.
- 2. Ethical and social responsibility** – there is now an expectation that organisations have safeguarding policies and practices in place, regardless of whether compliance or legislative requirements exist.
- 3. Risk mitigation strategies** – the safeguarding of vulnerable consumers involves detailed risk mitigation strategies. These plans should assess potential hazards, implement preventative measures, and provide a clear course of action to address incidents or cases.
- 4. Monitoring and reporting** – compliance monitoring and reporting ensure that all legal and regulatory compliance requirements are met. Compliance monitoring and reporting must be ongoing and ever-evolving alongside changes in the legal landscape.
- 5. Training and recruitment** – educating employees, contractors and volunteers on the complexities of safeguarding and the diverse needs of vulnerable groups is paramount. Recruitment strategies should be underpinned by a commitment to support vulnerable people.
- 6. Impact and recovery** – the impact of neglect or abuse on vulnerable people can be profound. Recovery-focused support systems are integral for healing and resilience. As part of their safeguarding strategy, organisations must review their impact and recovery approaches.
- 7. United Nations Sustainable Development Goals** – adopted by all United Nations Member States, the United Nations agenda sets out the plan to reach the 17 Sustainable Development Goals (SDGs) by 2030. The SDGs recognise the direction the world is heading in terms of addressing social needs including social protection and equal access for all.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

LEGISLATION, COMPLIANCE, AND DRIVERS

All directors and senior leaders have legal responsibilities to ensure the organisation meets the legislation and regulation in place to protect vulnerable people. In Australia, every organisation – regardless of their sector, industry, and services – have a role to play. In some cases, criminal sanctions may be imposed where reasonable steps are not taken to remove or reduce the risks posed to vulnerable people.

Over the years, a series of Royal Commissions have been conducted to investigate systemic issues, with a particular focus on the protection of vulnerable consumers and customers. If an organisation doesn't believe it has vulnerable consumers or customers, the recent Royal Commissions, and reviews across a wide range of sectors should convince them otherwise.

Notable among these is The Royal Commission into Institutional Responses to Child Sexual Abuse, which led to significant reforms and new child protection legislations across many industries. The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry exposed a range of misconduct and mistreatment against vulnerable consumers, leading to stricter financial industry regulations. Others include the Royal Commission into Aged Care Quality and Safety, the Royal Commission into the Robodebt Scheme, the Disability Royal Commission, and various mental health reforms. Each of these highlight the impacts of failing to identify and integrate customer vulnerability into organisations' operations.

The United Nations is also a key driver of the protection and safety of vulnerable people. The Sustainable Development Goals focus on specific themes of social deprivations and inequalities such as ensuring protection and good wellbeing for all at all ages (number 3) and ensuring equitable education opportunities for all (number 4). Additionally, The United Nations Convention on the Rights of a Child² and The Convention on the Rights of Persons with Disabilities³ are a good place for an organisation to start when reviewing their responsibilities and learning about these vulnerable groups with greater empathy and understanding.

It is important to note that vulnerability cannot always be observed and can often impact people in different ways. As an extension of those previously mentioned, key considerations, compliance areas and examples for the board to consider include, but are not limited to the below:

- 2 Unicef Australia, United Nations Convention on the Rights of the Child, https://www.unicef.org.au/united-nations-convention-on-the-rights-of-the-child?srsltid=AfmBOor6dSCrKpEOhSTPGDTd2q4DvYj5iNK_1bVGXes3OzHotEzn3_Nr
- 3 United Nations Enable, Convention on the Rights of Persons with Disabilities (CRPD), <https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-Disabilities.html#Fulltext>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

01. Child safety

The National Framework for Protecting Australia's Children 2021-2031 sets out the key priorities and focus areas for managing child protection issues in Australia. State and territory governments are responsible for legislation, including the *Children and Young Persons (Care and Protection Act) 1998* in New South Wales and *The Children, Youth and Families Act 2005* in Victoria.

- In the **real estate or retail sectors**, this may involve organisations protecting children in the shopping centres they operate.

02. Consumer protection

The Australian Consumer Law (ACL) protects vulnerable consumers from being negatively affected by unfair business practices, e.g. false, misleading, or deceptive conduct and coercion.

- In **financial services**, an example is a debt collection firm continually harassing and intimidating a resident in a care facility who has difficulty speaking after suffering an injury

03. Information sharing, privacy, and data protection

The *Privacy Act 1998* regulates how personal information is handled by government agencies, private sector organisations, and not-for-profit organisations. There are specific provisions on how to handle sensitive information, which can include information about children and other vulnerable individuals.

- For example, a healthcare **provider or medical services company** must allow individuals the option to interact anonymously or using a pseudonym where possible and feasible to protect the individual from harm including domestic or family violence.

04. Aged care and disability

The *Disability Services Act 1986* ensures that programs and services delivered to people with disabilities are provided in a way that supports their independence and participation in the community. The *Aged Care Act 1997* and its associated principles set out the responsibilities of aged care providers, the accreditation requirements, and the quality of care that must be provided.

- A **company that runs a network of aged care facilities**, must have processes in place to manage complaints effectively, provide appropriate care, and respect the dignity and privacy of each resident.

The above compliance areas explore some of the specific legal and ethical measures organisations must meet to protect vulnerable groups. Non-compliance can lead to significant legal consequences, reputational damage, and most importantly, harm to vulnerable groups of people that these rules and regulations aim to protect.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

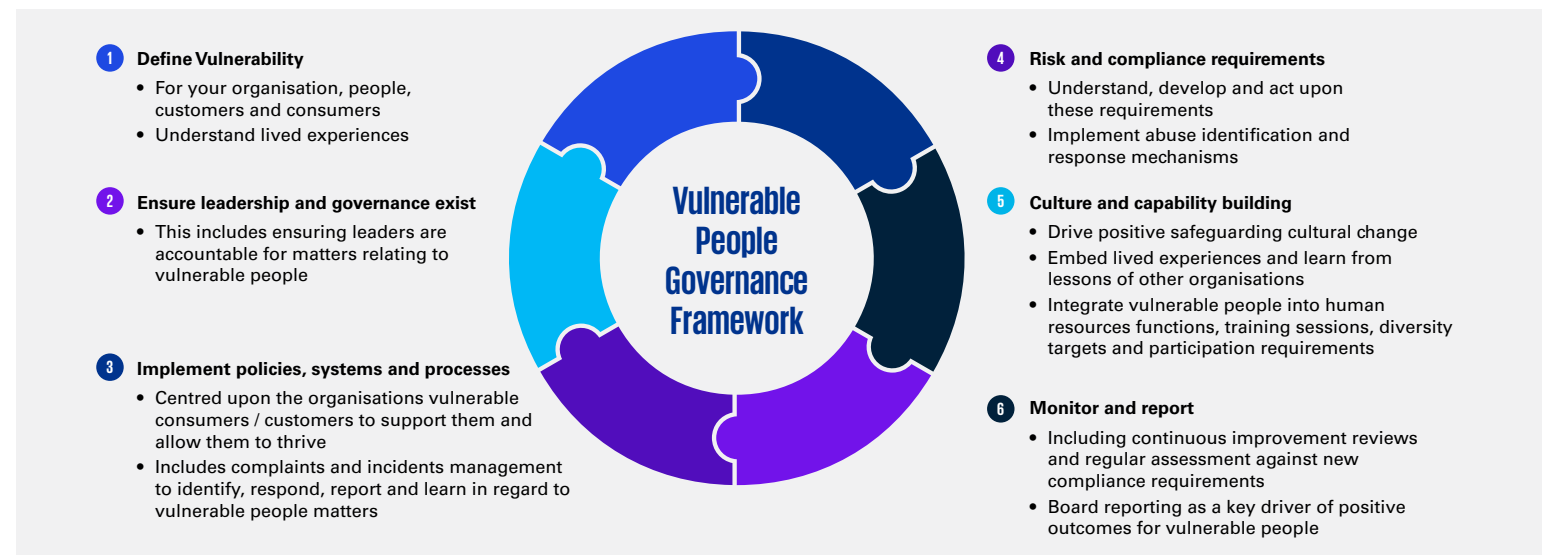
GLOSSARY

APPENDICES

CONTACT US

VULNERABLE PEOPLE GOVERNANCE FRAMEWORK

KPMG have developed a Vulnerable People Governance Framework to assist boards with developing their safeguarding governance strategy and to ensure their governance approach is exhaustive.



RISK AND MEASURES OF SUCCESS

Risk identification is crucial in the setting of safeguarding vulnerable people as it defines the actions to be taken by an organisation to ensure vulnerable people are protected from potential harm or abuse.

As defined by the National Office for Child Safety (NOCS), risk is defined as 'the possibility of something adverse happening the future'.⁴ As an example, and within the context of child safety, NOCS elaborates that to identify specific child safety risks, understanding the risk context is 'what allows different sizes and types of organisations to understand their parameters and tailor

risk management to fit their context'.⁵ This concept can be applied more broadly to identify risks for other vulnerable populations and highlights that recognising risks and their context, affect how an organisation can reach its social, ethical, and legal objectives.

Vulnerable people must be considered and embedded into all risk management practices. Refer to [Chapter 17 Risk Management](#), for more information.

To have a full understanding of the risks to the organisation, its clients and its stakeholders, directors may consider following a similar step-by-step approach to identify and classify its risks. Directors should also examine what the sources of risks are and how to mitigate them through established risk management frameworks.

⁴ National Office for Child Safety, 'Child Safety Risk Management Guide: Upholding the rights of children and young people', (Commonwealth of Australia, 2023), <https://www.childsafety.gov.au/system/files/2023-07/child-safety-risk-management-guide.pdf>, 9.

⁵ National Office for Child Safety, 'Child Safety Risk Management Guide', 13.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Measures of success or key risk indicators (KRIs) should be decided upon for each identified risk. KRIs can be any positive, neutral, or negative performance metric which provides information on how the risk is tracking. KRIs can be used by all organisations once risks have been identified and documented.

Example of measures of success/KRIs for risks related to vulnerable people include:

- number of policy breaches
- timeliness of complaint resolution
- number and trends of incidents (both major and minor) related to vulnerable people
- number of employee or volunteers recruited without proper screening or safety checks, e.g. Working with Children Checks
- number of complaints received regarding staff misconduct including bullying or discrimination
- employee training completion results
- consumer survey results or Net Promoter Score, e.g. measuring individual consumers' awareness of their rights and responsibilities.

Measures may not be as immediately straightforward as they seem. For example, more complaints may not demonstrate a lack of progress, but may instead show that the organisation has an effective complaints system and reporting culture, and conversely few complaints may be a sign of a lack of opportunity or understanding of how to raise a safety-related concern.

THE ROLE OF THE BOARD

The board holds a central role in embedding ESG principles, with a focus on safeguarding vulnerable people. Boards are ultimately held accountable for driving an organisation and a culture where safeguarding and safety of vulnerable customers, consumers and communities is at the heart of its operations, ensuring the risk of harm and abuse to vulnerable consumers is minimised or where possible, non-existent.

Leadership must be comprehensive in integrating and overseeing all safeguarding-related matters to sufficiently mitigate potential and existing risks faced by vulnerable people. Appropriate mechanisms must be in place to facilitate escalation of serious incidents, risks and complaints to the board.

Incorporating safeguarding into the organisational strategy is one of the first steps an organisation must take to commence its safeguarding journey.

In our experience, boards should start with the below:

- 1. Take responsibility and accountability for safeguarding** within their organisation by elevating this topic to a governance priority and ensure that all consequent responsibilities are effectively distributed throughout the organisation.
- 2. Understand where your organisation serves and supports vulnerable people**, how your vulnerable customers are identified, served and supported across the customer journey.
- 3. Understand and comply with relevant laws and regulations** related to safeguarding, child safety and vulnerable adults.
- 4. Complete holistic reviews and a gap analysis on safeguarding practices** within the organisation to identify all current gaps or risks.
- 5. Develop comprehensive policies and targets** that reflect an ongoing commitment to protecting and caring for all potentially impacted vulnerable groups.
- 6. Ensure safeguarding measures, reporting mechanisms and protective frameworks are in place** and linked to the strategic vision.
- 7. Provide clarity on the short, medium, and long-term direction of safeguarding practices** to ensure a more detailed framework and comprehensive policies can be developed.
- 8. Ensure you are receiving safeguarding-related board reports and evaluations** – this includes challenging the organisation to continuously refine and improve their safeguarding evaluations and assessments.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

9. Oversee the organisation's risks relating to safeguarding

including the risk tolerance, controls, measures, and financial and non-financial assessments of these.

10. Create or re-enforce an organisational culture that will assist with delivering and embedding positive safeguarding-related change that is focused on continuously improving.**11. Challenge the performance of the organisation** in alignment to its safeguarding KPIs, targets and KRIs.**12. Engage in regular training and capability building** to stay current with safeguarding-related matters and continuously challenge leadership on their frameworks and processes.

Regular reporting to the board on the organisation's safeguarding risks enables the board to make changes that deeply impact the long-term sustainability and resilience of the organisation. Areas to be considered when reporting include:

1. Progress against safeguarding objectives and strategy.
2. Safeguarding metrics and data documenting lead and lag indicators to indicate the achievement of the organisation's safeguarding strategic priorities.
3. Performance against key risk/performance indicators designed in relation to safeguarding.
4. Legislative and regulatory updates, breaches and policy breaches including employee code of conduct breaches.
5. Risk assessments and the strategic risk profiles relating to the safeguarding of vulnerable people.
6. Status of high-risk incidents and complaints, and how these may lead to changes in existing policies.
7. Regular review and status of governance frameworks, policies, and procedures.
8. Risk management plan progress including the outcomes of risk monitoring which may identify new risks.
9. Training and education outcomes of staff and management.

Building board confidence

A critical aspect of building board confidence is engaging in ongoing capability uplifts and updates which provide an understanding of the ever-evolving risk environment and legislation that underpins the safe treatment of vulnerable customers and consumers.

Board confidence will exist when there is regular action, conversation and change built upon the safeguarding of its vulnerable customers and consumers.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- Australian Government, <https://www.legislation.gov.au/C2018A00149/latest/versions>
- Royal Commissions. n.d. *Recent Royal Commissions*, <https://www.royalcommission.gov.au/recent>
- Department of Home Affairs, <https://www.homeaffairs.gov.au/about-us/our-portfolios/multicultural-affairs/about-multicultural-affairs/access-and-equity>.
- National Office for Child Safety. 2023. *Child Safety Risk Management Guide*, <https://www.childsafety.gov.au/system/files/2023-07/child-safety-risk-management-guide.pdf>
- United Nations Convention on the Rights of the Child, United Nations Convention on the Rights of the Child ([unicef.org.au](https://www.unicef.org.au))
- United Nations Convention on the Rights of Persons with Disabilities, Convention on the Rights of Persons with Disabilities (CRPD) | United Nations Enable
- United Nations Sustainable Development Goals, THE 17 GOALS | Sustainable Development ([un.org](https://www.un.org))

For further information please contact:



Dr Meg Brodie

Partner in Charge, ESG Social
KPMG Australia
megbrodie@kpmg.com.au

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

20. Private Equity

Private equity led public to private transactions have increased in frequency and are now being transacted with heightened corporate governance expectations. Directors operating in this environment will need to understand their governance responsibilities, issues and priorities.

In this chapter

- What is private equity?
- Pre-private equity considerations for boards
- PEC board considerations

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Are there protocols for managing conflicts of interest with participating directors and/or management?
2. Does the board understand the potential personal financial upside to management from a private equity (PE) deal?
3. Are protocols in place to secure independent review of any approach?
4. Should the board set up an independent subcommittee to lead decision-making and process-manage a potential transaction?
5. Does the board understand the position of key shareholders?
6. Should a broader sale process be initiated to maximise shareholder value?
7. Is the board clear on its requirements regarding when and what to disclose to the markets?
8. Does the board have a 'defence protocol' for a potential approach by a prospective bidder that enhances the company's responsiveness and mitigates potential risks?
9. Does the board discuss the approach or the proposed transaction in closed sessions without participating directors and management?
10. What will the impact of the PE approach have on the board's normal agenda?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The board has in the past been caught unaware by PE bids.
- No strategy has been developed for dealing with PE bids and it is rarely discussed at board meetings.
- Continuous disclosure issues have been raised against the company over past PE bids.
- Directors' messages are inconsistent or unclear regarding their position on PE bids.
- Independent advisers are not engaged to examine PE submissions.
- Disclosure of directors and senior managements' interests is not clear.
- A lot of work needs to be undertaken for the company's financial, operational and commercial information to stand up to a due diligence process.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

WHAT IS PRIVATE EQUITY?

The term private equity (PE) covers a broad range of activities related to investing in unlisted companies. It may include taking listed companies private. It represents an alternative model to that of the dispersed ownership of a publicly listed entity.

At the end of 2023, the combined value of Australian private equity and venture capital assets under management totaled \$65.5 billion,¹ up 30 percent over an 18 month period, with approximately a third of assets under management sitting as 'dry powder' for future transactions. The increase in the value of assets under management reflects an active period of new fund raising over 2021 and 2022, together with period of lower transaction activity in 2023.

PRE-PRIVATE EQUITY CONSIDERATIONS FOR BOARDS

Boards need to be on the front foot when PE does come knocking. A plan of action developed beforehand regarding how to respond to a bid, be it from PE or anyone else, is a good idea.

Boards must not be too hasty in rejecting an informal takeover approach. Those who dismiss informal takeover approaches without engaging further (for example, seeking to negotiate an improvement in price and conditions) because they believe the indicative offer price is inadequate – only to find that industry conditions deteriorate or other circumstances arise that adversely impact the successful execution of their current strategy – leave themselves exposed to shareholder criticism. Pressure then mounts on the board to defend their earlier decision to not engage with the proponent of the informal takeover approach.

Failure to achieve a materially better outcome for shareholders within a reasonable time of rejecting an indicative takeover proposal can attract further criticism from shareholders, with reputational implications for the directors.

A board cannot leave the initial response to a PE approach to management, which is very likely to possess a conflict through its involvement in the transaction via a management buyout.

The board's fiduciary duty is to continue to act in the best interests of shareholders as a whole. Directors should consider:

- understanding whether the PE approach is a 'sounding out' conversation or an immediate precursor to a bid
- obtaining market perceptions reports
- procuring up-to-date valuations (can set the tone for subsequent negotiations and discussions)
- arranging a panel of selected advisers (speaking with them in closed sessions without management)
- ensuring policies are appropriate and clear (e.g. conflict of interests)
- setting ground rules (roles and responsibilities) for the board, chair, board committee and individual director involvement
- understanding the shareholder base (current and future) and the role a PE investor might have as a potential source of funding for future growth and expansion strategies
- establishing a due diligence process, particularly around the degree of access, if any, that may be granted to this or any other bidders, and areas of possible synergies from merging with potential bidders (which may be part of a defence/price maximisation strategy)
- providing institutional investors with enough information for them to do their own valuations.

Despite the focus and commitment in dealing with a PE approach, it will be business as usual at the frontline. The board also needs to consider the impact of an approach on its normal agenda. To assist with this, and to isolate directors who may have a conflict of interest, an ad hoc board committee can take control of the company's response to a PE offer.

¹ Australian Private Capital Market Overview: A Preqin and Australian Investment Council Yearbook 2024, https://investmentcouncil.com.au/common/Uploaded%20files/Preqin/2024Yearbook/2024_Australian_Private_Capital_Market_Overview.pdf.pdf

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

This board committee should:

- comprise independent directors who are free of conflicts
- possess access to its own advisers who are also free of conflicts
- have appropriate authority
- pay careful attention to the documentation presented and produced (and if necessary, have the authority to obtain an independent fairness opinion/valuation)
- tightly monitor continuous disclosure and any transparency issues with price sensitive information during the transaction (including decisions on when to go public and the control and provision of confidential information by independent directors to the board and management)
- continuously monitor the market for other possible opportunities.

The committee needs to be open-minded, willing to take advice, and consider all options and alternative strategies (defence strategies, further independent valuation, auction strategies and overcoming impasses).

The existence of the committee does not, however, relieve other directors of their obligations under the Corporations Act and ASX Listing Rules during PE activity. The key objective is to provide good counsel to shareholders on the PE proposal.

PEC BOARD CONSIDERATIONS

In principle, Private Equity Committees (PEC) should observe many of the same governance practices adhered to by publicly listed companies.

The PEC board is typically structured in the best interests of the investee company. The composition of the PEC board will inevitably change with greater representation from the PE investor. Good practice includes maintaining an independent chair and ensuring that a majority of directors are independent. A PEC board consequently tends to be smaller due to the high cost of appointing independent non-executive directors. However, board appointees should continue to be individuals of appropriate competencies, skill and experience who can provide value and insight to the PEC. The relationship between the board and management should be clear and be supported by the

appropriate documentation of roles and responsibilities, with effective conflict of interest policies. In some cases, the board develops and monitors a 'management agreement' between the investors, the board and management to assist this cause. The board's charter depends on what the PE owners expect. This may also be dependent on what the lender(s) demand. Some roles and responsibilities may also change (e.g. audit committee, company secretary, etc.).

As many PECs eventually re-emerge as publicly listed entities, PEC boards will be better served if their governance frameworks allow a seamless transition to public trading.

Useful resources

- Australian Investment Council, <https://investmentcouncil.com.au/AIC/>
- Australian Private Equity & Venture Capital Journal, <https://www.privateequitymedia.com.au/journal/>
- Australian Investment Council 2023 Annual Report, <https://investmentcouncil.com.au/AIC/Articles/Media-Release/2023/2023-Annual-Report>

For further information please contact:



James Hindle

Private Equity Sector Leader
KPMG Australia
jhindle@kpmg.com.au

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

21. Health, Safety and Wellbeing

Every workplace is exposed to occupational health, safety and well-being risks, regardless of the industry they operate within. Employers (including Boards and Directors) are responsible for the health and safety of all workers and other parties impacted by their activities and operations. Health and safety is fundamental for all organisations and begins with Board leadership. Organisations should ensure they have robust systems and processes in place to facilitate compliance with Work Health and Safety (WHS) legislation and to effectively manage and mitigate health and safety risks so far as is reasonably practicable.

In this chapter

- Key concepts – health, safety and wellbeing
- Legislation
- Strategy
- Governance
- Organisational structures
- Due diligence
- Penalties
- Performance management
- What health and safety information should be provided to the board?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Does the Board have oversight of a clear health, safety and wellbeing strategy, together with defined and measurable performance indicators and targets? Are these targets fit for purpose and able to be measured and tracked effectively?
2. How does the Board hold management accountable for implementing the health, safety and wellbeing strategy and policy, and ensure that the CEO meets the Board's expectations?
3. How does the Board demonstrate its commitment to a positive health, safety and wellbeing culture?
4. Does the Board understand the legalities of the health, safety and risk environment in which they operate?
5. Has the Board received the appropriate training to enable it to meet due diligence obligations and ask the right questions to effectively challenge health, safety and wellbeing performance?
6. Is there a proactive, risk-aware culture where leaders value and prioritise health, safety and wellbeing within the organisation?
7. What audits, reviews or assessments are undertaken to provide assurance over health, safety and wellbeing management processes and performance?
8. How does the Board ensure that it is kept informed of relevant health, safety and wellbeing information and that risks are escalated from management or other parties?
9. What meaningful information does the Board receive about health, safety and wellbeing performance to inform risk-based decision-making?
10. Do Directors understand their liabilities and responsibilities when it comes to ensuring the health, safety and wellbeing of workers and how is this demonstrated?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- There is a lack of board-level objectives and targets for health, safety and wellbeing and/or the targets in place do not use the SMART principles for measuring objectives and targets.
- There is no vision/strategy or annual health, safety and wellbeing plan.
- There is a lack of board oversight or appropriate level of engagement in the determination, development, endorsement, promotion and/or review of the organisation's health, safety and wellbeing strategy and policies.
- Health, safety and wellbeing information does not appear on the agenda for board meetings.
- Board members have not received appropriate information and training on their health, safety and wellbeing responsibilities.
- Board reporting of health and safety performance is based only on lag indicators (e.g. number of incidents / injuries) rather than lead indicators (e.g. number of risk assessments, risk control effectiveness, training and education, leadership engagement, worker safety suggestions, and other proactive measures to manage health, safety and wellbeing issues).
- Where there has been significant organisational change, the implications for health, safety and wellbeing have not been reported to the board.
- The company continues to have poor health, safety and wellbeing outcomes despite management's assurance that 'appropriate and effective' controls are in place.
- Contradictory/counterperformance indicators are being reported (e.g. workers compensation claims costs; and the frequency and duration of injuries are escalating yet other safety key performance indicators, such as lost time injury frequency rates, are improving).
- Material health, safety and wellbeing risks are ignored or undisclosed (e.g. contractor performance is ignored, where contractors contribute to the workforce, or where the company has overseas operations, these risks are undisclosed/ignored in reporting).
- Health, safety and wellbeing risks are not considered or existing risks are not adequately risk assessed within the organisation's risk management framework.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

KEY CONCEPTS – HEALTH, SAFETY AND WELLBEING

Organisations have a duty of care to ensure that any person affected by the company's undertakings remains safe at all times and their work activities are not prejudicial to their health – or the health of others.

Health, safety and wellbeing extends not only to the physical safety of the workforce, but also to mental health and wellbeing. Having a strong health and safety culture, and an embedded and effective management system by which managers and workers demonstrate accountability, can result in significant benefits for an organisation. The failure of organisations to effectively manage health, safety and wellbeing risks and performance has both human and business costs and, as such, should receive the same priority by directors as all other risks.

Health, safety and wellbeing governance is as important as any other aspect of governance and is both core to an organisation's overall risk management function and a key responsibility of directors. This approach includes change to hazard identification, evaluation and control of risks and threats to the health, safety and wellbeing of workers, communities and supply chains.

PSYCHOSOCIAL RISK MANAGEMENT

Psychosocial risk refers to workplace hazards that have the potential to cause psychological harm (regardless of whether they also cause physical harm). Psychosocial risks may arise from hazards related to the design or management of work, a work environment, the physical workplace or workplace interactions and behaviours. The source of psychosocial hazards is broad however, they primarily arise from or are related to:

1. the design and management of work, including lack of role clarity, unachievable or unreasonable job demands, low job control, poor support or inadequate reward and recognition
2. interactions at work, including harassment, sexual harassment, bullying and conflict and poor workplace relationships

3. the conditions or environment in which work is done, including poor organisational change management, remote or isolated work and poor physical environments
4. lived experiences at work, including poor organisational justice, violent and aggressive behaviours, traumatic events or exposure to harmful material.

Psychological wellbeing is a safety issue and a priority enterprise risk, and psychosocial risks must be managed with the same rigor as physical risks. Boards and Directors need to be aware of potential organisational hazards and take reasonable steps to verify that resources, systems and procedures to manage psychosocial risk are provided, used and monitored for effectiveness. Directors must understand their obligations and act to ensure they are protecting workers and their organisation from these risks and avoiding penalties associated with regulatory non-compliance.

Duty of care

An organisation must take reasonably practicable steps to ensure that workers and other persons are not exposed to risks to their psychological or physical health and safety. An organisation must eliminate psychosocial risks in the workplace or minimise these risks.

Operational risks

Psychosocial risks cause significant harm to people, including psychological and physical harm. In turn, this leads to an erosion of workplace culture, impacting on the organisation's ability to attract and retain talent.

Financial and legal risks

Incidents arising from psychosocial risks negatively impact profitability, labour and operational costs and revenue. Publicly reported incidents impact market value and can result in significant legal and financial penalties on organisations and Directors.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Since 2017-2018, there has been an increase in claims associated with work related mental health conditions by 36%.¹ The median compensation paid for mental health claims in 2020-2021 was \$58,000. This is almost four times the median compensation paid across all claims. Psychological injury claims result in significantly higher costs and time off work for employees, compared to physical WHS claims.

Governance risks

Directors have governance responsibilities and can strongly influence the culture and accountability of the organisation through their behaviour. Directors can also influence critical decisions about the deployment of resources for managing psychosocial risk and sexual harassment, and the development and implementation of policies and processes to support organisational compliance with relevant legislation.

Directors must consider the broader intention of regulatory requirements – to protect the health, safety and wellbeing of people. To meaningfully address workplace psychosocial risk, leaders need to address the underlying systemic drivers of harm and not engage in compliance as a 'box-ticking' exercise. To set the tone from the top, Boards and Directors must prioritise these issues, ask questions and regularly seek information and specific data and reporting on relevant areas of investigation.

Directors must also understand the skillset required to conduct psychosocial risk assessments and the steps necessary to control these risks. The organisational contributors to psychosocial hazards are different and often more challenging to review and assess compared to physical hazards. Psychosocial hazard management requires a deep understanding of the organisation, its operations, leadership and workplace culture, as well as emotional intelligence to understand the cause and effect of the risk. Directors need ensure that management, HR, WHS and risk personnel are equipped with the necessary skills to address organisational and systemic drivers of psychosocial harm.

¹ Safe Work Australia, Australian Work Health and Safety (WHS) Strategy 2023–2033: Baseline report on targets, 2024

LEGISLATION

All directors have a legal imperative to ensure that the organisation which they represent remains compliant with relevant health and safety legislation.

In Australia, nationally harmonised health and safety legislation is in effect in most Australian states and all territories. Harmonisation is based on the development of the Model Work Health and Safety Act 2011 and Model Work Health and Safety Regulations 2011 (collectively, the model WHS laws). The model WHS laws outline the key aspects of health and safety legislation that each State and Territory then adopts into their respective WHS legislation. Safe Work Australia does not regulate state and territory WHS laws, which remains the responsibility of the relevant regulators in each jurisdiction.

The model WHS laws have been adopted by all states and territories, as reflected in their respective legislation, except for Victoria. Victoria has not amended its legislation, as its existing laws (the Occupational Health and Safety Act (OHS Act) 2004) are already considered reflective of nationally harmonised standards.

The alignment between the WHS Act, the OHS Act 2004 in Victoria, and the Commonwealth Corporations Act 2001 (the Corporations Act) underscores the shared emphasis on accountability, due diligence, and governance in managing workplace health and safety. While the WHS Act provides a harmonised framework across most Australian jurisdictions, the OHS Act 2004 reflects Victoria's independent approach. The Corporations Act complements these frameworks by embedding health and safety compliance into broader corporate governance responsibilities. Together, these legislative instruments establish a robust foundation for Officers to ensure workplace safety and uphold their governance duties.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

OFFICERS' DUTIES

- **WHS Act:** Officers under the WHS Act are required to ensure compliance with health and safety obligations as part of their governance responsibilities. This includes understanding the operations of the business and its associated risks.
- **OHS Act 2004:** In Victoria, the OHS Act places similar duties on Officers, requiring them to ensure the organisation provides a safe working environment and maintains safe systems of work. However, the OHS Act does not adopt the 'Person Conducting a Business or Undertaking' (PCBU) terminology used in the WHS framework.
- **Corporations Act:** Officers must act in good faith, with care and diligence, and in the best interests of the company, ensuring compliance with all applicable laws, including health and safety legislation.

DUE DILIGENCE REQUIREMENTS

- **WHS Act:** Officers must exercise due diligence by:
 - Acquiring and maintaining knowledge of WHS matters.
 - Understanding the nature of the business and its risks.
 - Ensuring adequate resources and processes are in place to mitigate risks.
 - Monitoring and verifying compliance with WHS obligations.
- **OHS Act 2004:** While the OHS Act does not explicitly outline 'due diligence' in the same terms, it requires Officers to proactively ensure compliance with health and safety obligations, which aligns with the principles of due diligence under the WHS Act.
- **Corporations Act:** Officers are required to exercise care and diligence in fulfilling their governance responsibilities, which includes ensuring compliance with health and safety laws.

INDUSTRIAL MANSLAUGHTER

- **OHS Act 2004:** Victoria's OHS Act includes specific industrial manslaughter provisions, with penalties of up to 25 years imprisonment for individuals and fines of up to \$16.5 million for corporations. These provisions are among the most stringent in Australia and aim to deter breaches leading to workplace fatalities.
- **WHS Act:** Other jurisdictions under the WHS framework also include industrial manslaughter provisions, but the penalties and definitions vary.
- **Corporations Act:** While the Corporations Act does not directly address industrial manslaughter, it holds Officers accountable for breaches of their governance duties, which may include failures related to workplace safety.

GOVERNANCE AND ACCOUNTABILITY

- **WHS Act:** Health and safety compliance is a critical component of corporate governance, requiring Boards and Officers to integrate WHS considerations into their broader governance responsibilities.
- **OHS Act 2004:** The OHS Act emphasises proactive measures by employers and Officers to ensure compliance, complementing the governance focus of the Corporations Act.
- **Corporations Act:** Officers are accountable for ensuring the organisation's compliance with all applicable laws, including health and safety legislation, as part of their broader governance responsibilities.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Model laws and regulation			Statutory authority
Model Work Health and Safety Act 2011 Model Work Health and Safety Regulations 2011			
Jurisdiction	WHS Legislation and Regulations	Psychosocial Regulations & Relevant Codes	Regulator
Federal	Work Health and Safety Act 2011 (Cth) Work Health and Safety Regulations 2011 (Cth)	Incorporated into WHS Regs 2011 (Cth) Supported by Safe Work Australia's Code of Practice on Managing psychosocial hazards at work	
NSW	Work Health and Safety Act 2011 (NSW) Work Health and Safety Regulation 2017 (NSW)	Incorporated into WHS Regs 2017 (NSW) Supported by Code of Practice on Managing psychosocial hazards at work	
QLD	Work Health and Safety Act 2011 (Qld) Work Health and Safety Regulation 2011 (Qld)	Incorporated into WHS Regs 2011 (QLD) Supported by Code of Practice on Managing psychosocial hazards at work	 WorkSafe qld.gov.au
ACT	Work Health and Safety Act 2011 (ACT) Work Health and Safety Regulation 2011 (ACT)	Incorporated into Work Health and Safety Regulation 2011 (ACT) Supported by Code of Practice on Managing psychosocial hazards at work	WORKSAFEACT SAFE + HEALTHY WORKPLACES
SA	Work Health and Safety Act 2012 (SA) Work Health and Safety Regulations 2012 (SA)	Incorporated into Work Health and Safety Regulations 2012 (SA) Supported by Code of Practice on Managing psychosocial hazards at work	 SafeWork SA
NT	Work Health and Safety (National Uniform Legislation) Act 2011 (NT) Work Health and Safety (National Uniform Legislation) Regulations 2011 (NT)	Incorporated into Work Health and Safety (National Uniform Legislation) Regulations 2011 (NT) Supported by Code of Practice on Managing psychosocial hazards at work	NT WorkSafe
TAS	Work Health and Safety Act 2012 (Tas) Work Health and Safety Regulations 2012 (Tas)	Incorporated into Work Health and Safety Regulations 2012 (Tas) Supported by Code of Practice on Managing psychosocial hazards at work	 Work Safe TASMANIA
VIC	Occupational Health and Safety Act 2004 (Vic) Occupational Health and Safety Regulations 2017 (Vic)	Occupational Health and Safety Amendment (Psychological Health) Regulations 2021 (Vic) Supported by Code of Practice on Managing psychosocial hazards at work	Work Safe VICTORIA
WA	Work Health and Safety Act 2020 (WA) come into effect in 2022. Work Health and Safety Regulations 2022	Incorporated into WHS Regulations 2022 (WA) Supported by Code of Practice on Managing psychosocial hazards at work	

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

STRATEGY

It is the duty of the Board to ensure that the organisation has the right strategic direction for health, safety and wellbeing. This must be underpinned by robust systems, processes, safety culture and the requisite resources and capability. Ultimately, Boards are responsible for determining the organisation's health, safety and wellbeing strategy and policy. The health, safety and wellbeing strategy and policy should also include consideration of all persons impacted by the organisation's activities, such as contractors and visitors, not just workers, contractors and visitors). However, Board responsibility should go beyond the issuing of strategy and policy. It should extend to ensuring the effective implementation of the health safety and wellbeing framework by holding management accountable through planning, implementation, monitoring and review.

Comcare (the Commonwealth WHS regulator for in Federal workplaces) states that a 'strong health and safety culture is key to profitability, sustainability, reduced compensation costs and other success measures. With an ageing workforce, the impact of chronic disease in the workplace and a competitive labour market, businesses using targeted strategies to build (and embed) health and wellbeing at work will have greater business performance and people outcomes' and that 'measuring health and safety performance provides an insight into management and investment decisions'. Senior leadership has a duty to ensure their organisation complies with its duties and obligations under the WHS Act and the Safety Rehabilitation Compensation Act 1988, which is responsible for establishing the national workers compensation scheme). Leadership has a duty to ensure work health and safety laws are appropriately and effectively integrated into everyday business. As part of the strategic direction, Directors should consider and challenge the key performance indicators that underpin the company's strategy. For example, safety performance (particularly numbers of/nature of incidents) is often reported by management, yet there is little to no disclosure on health indicators and associated impacts (mental and physical wellness), which often have a much greater effect on a business performance.

Culture, standards and values

The Board should take ownership for key health and safety issues and be ambassadors for good health and safety performance across the organisation. Boards achieve this by upholding core values and standards, setting the 'tone at the top', 'walking the talk' and establishing and promoting a positive culture across the organisation with a high level of communication on all matters concerning health and safety.

Strategic implications

The Board is responsible for driving the health, safety and wellbeing agenda. They have oversight and an understanding of the risks and opportunities associated with health, safety and wellbeing, including any market pressures which could compromise the organisational values and standards – ultimately establishing a strategy to respond and safeguard the organisation from risk.

Performance management

The Board should ensure they retain oversight of the key objectives and targets for health and safety management and create an incentive structure for senior executives which drives good health and safety performance, balancing both leading and lagging indicators, and capturing both tangible and intangible factors.

Internal controls

The board should ensure health and safety risks are adequately managed and controlled, and that a framework is established to ensure compliance with the core standards. It is important that governance structures enable management systems and processes, actions and levels of performance to be challenged. This process should utilise, where possible, existing internal control and audit structures, and be reviewed by the audit committee, or other suitable committee or board members, where necessary.

Recommendation 7.1 of the ASX Principles suggests that listed entities have a dedicated risk committee (which may be a combined audit and risk committee), addressing different elements of risk.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Most organisations include oversight of health, safety and wellbeing risk in the remit of the risk committee. In the absence of a risk committee, many organisations establish a dedicated committee to specifically oversee health, safety and wellbeing risks. These often include environmental and/or community risks as well (Health, Safety, Environment and Community (HSEC) committee). Under WHS legislation, a health and safety representative (also known as HSR) can request to establish a Health and Safety Committee providing it meets certain requirements as set out in the WHS legislation. The function of the committee is to help facilitate cooperation and consultation with work groups and/or through their HSRs in health and safety matters.

GOVERNANCE

Director competence

All directors should have a clear understanding of the key health, safety and wellbeing issues characterising their organisation and be continually developing their skills, knowledge and understanding in this area. Knowledge of good health and safety governance structure and practice includes but is not limited to the following:

- liability of directors and industrial manslaughter offences
- workplace health and safety duties and obligations under the WHS Act
- due diligence – what is it and how do you demonstrate it
- understanding the hazards and risks of business operations
- knowing WHS performance metrics – leading and lagging
- leadership and culture
- systems and processes for managing health, safety and wellbeing risks.

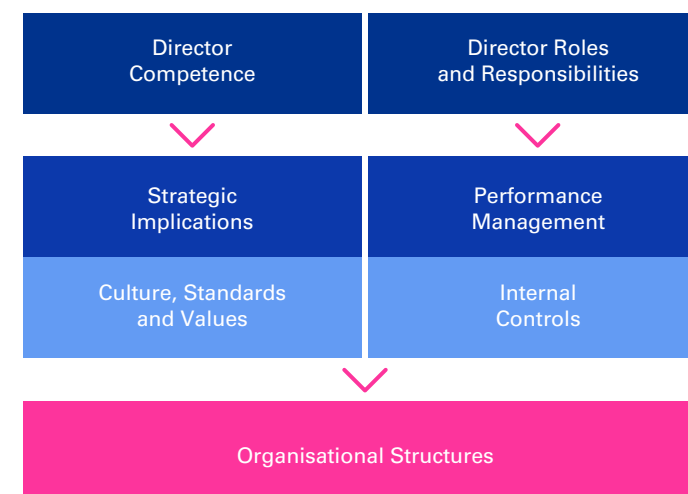
Director roles and responsibilities

All directors should understand their legal responsibilities and their role in governing health, safety and wellbeing matters for their organisation. Their roles should be supported by formal individual terms of reference, covering (at a minimum) the oversight of the health, safety and wellbeing strategy development, setting of policies and standards, performance monitoring and oversight of an internal controls framework. Where applicable, directors should communicate to all levels in the organisation or within their scope of direct reports about their specific health and safety responsibilities, authority to act and reporting requirements.

ORGANISATIONAL STRUCTURES

The board should integrate health, safety and wellbeing governance processes into the organisation's broader corporate governance structures, including the activities of the main board and its committees. In some cases, the creation of an additional board committee to consider health, safety and wellbeing matters may be relevant (as discussed above).

Better practice framework for WHS governance



FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

DUE DILIGENCE

Regardless of the size of the undertaking or the nature of the organisation's health, safety and wellbeing risk profile, it is important that directors, as officers, are fully informed of the relevant health, safety and wellbeing matters, up-to-date key information (e.g. COVID-19 changes) and the requirements that apply to them. This includes understanding their role in governing health, safety and wellbeing, as part of their broader responsibilities of good corporate governance.

Under WHS laws, the exercise of due diligence is the individual obligation of each officer or 'person conducting a business or undertaking' (PCBU). This means that each individual officer should consider how they will demonstrate compliance with their due diligence requirements contained in the WHS Act.²

How do directors/officers demonstrate due diligence?

In exercising due diligence, section 27 of the WHS Act requires officers to show that they have taken reasonable steps to:

1. acquire and keep up-to-date knowledge of work health and safety matters

2. gain an understanding of the nature of the operations of the business or undertaking of the PCBU and generally of the hazards and risks associated with the operations
3. ensure the PCBU has available for use, and uses, appropriate resources and processes to eliminate or minimise risks to health and safety arising from business operations
4. ensure the PCBU has appropriate processes in place for receiving and considering information regarding incidents, hazards and risks and responding in a timely way to that information
5. ensure the PCBU has, and implements, processes for complying with any duty or obligation of the PCBU under the WHS Act
6. verify the provision and use of the resources and processes referred to in points 3 to 5 above.

PENALTIES

In Australia, significant personal penalties apply to a corporation, officer or PCBU who fails to exercise due diligence under the WHS Act (in the relevant jurisdictions to which the WHS Act applies). The individual penalties for a breach are:

Type of offence	Maximum penalty for corporation	Maximum penalty for officers	Maximum penalty for workers
Category 1 offence – recklessness that leads to serious injury or death	\$3,000,000	\$600,000 or 5 years imprisonment	\$300,000 or 5 years imprisonment
Category 2 offence – failure to comply with the duty leads to serious injury or death	\$1,500,000	\$300,000	\$150,000
Category 3 offence – simple failure to comply with the duty	\$500,000	\$100,000	\$50,000

² Refer to Safe Work Australia, 2019, Model Work Health and Safety Bill, <https://www.safeworkaustralia.gov.au/system/files/documents/2003/model-whs-bill9-december2019.pdf>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Similar penalties apply in Victoria and Western Australia subject to the provisions of the relevant health and safety legislation in those jurisdictions.

Industrial manslaughter in Australia

Industrial manslaughter refers to the offence where a person conducting a business or undertaking (PCBU) has recklessly or negligently failed to ensure the safety of workers, or others impacted by their business or undertaking, leading to a death. In this instance, a Director may also be liable if found to have significantly contributed to a workplace fatality through negligence or failure to meet their WHS obligations.

Industrial manslaughter laws aim to prevent workplace deaths and deter employers from breaching health and safety duties owed to workers and others. Directors must understand how and why industrial manslaughter offences can arise and take the necessary steps to establish appropriate and effective work health and safety systems. Industrial manslaughter offences are now passed in all Australian States and Territories. The individual and body corporate penalties for industrial manslaughter are:

	Maximum penalty for individual	Maximum penalty for a body corporate
New South Wales	25 years imprisonment	\$20,000,000
Victoria	25 years imprisonment	\$19,759,000
Queensland	20 years imprisonment	\$13,345,000
Australian Capital Territory	20 years imprisonment	\$12,025,000
Northern Territory	Life imprisonment for an individual	\$12,025,000
Western Australia	20 years imprisonment \$5,000,000 fine for an individual	\$10,000,000
Tasmania	20 years imprisonment	\$18,000,000
South Australia	20 years imprisonment	\$18,000,000

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

WHS exemption from D&O insurance

Importantly, there is a permanent exemption from D&O insurance for WHS obligations. Under WHS legislation, an officer or PCBU cannot delegate to another person or company their obligation to devise, maintain and implement a safe and proper system of work. Consequently, directors cannot insure against negligence.

Examples of WHS convictions

Date of conviction	Incident Description	Conviction
WA 2025	An employee working as a plant operator was fatally injured whilst working in a processing facility. Breach – being a person with management or control of fixtures, fittings or plant at a workplace, did not, so far as is reasonably practicable, ensure that the fixtures, fitting or plant were without risks to the health and safety of any person, and by that contravention caused the death of a person.	Company convicted and fined \$875,000
VIC 2025	A government department was charged with failing to comply with its primary health and safety duty under the WHS Act when an employee was stabbed by a member of the public. It was alleged that the department failed to implement adequate security measures, such as providing sufficient uniformed security guards and managing entry protocols, to prevent the risk of physical violence to workers.	The employer faces a maximum fine of \$1.5M
QLD 2025	A company was sentenced for breaching section 32 of the WHS Act, having failed to comply with its primary health and safety duty, resulting in an explosion which caused the death of a worker, and serious physical and psychological harm to 3 other workers.	Employer convicted and fined \$400,000
WA 2024	An employee suffered serious psychosocial harm when the employer, a government department, failed to provide and maintain a safe work environment. The harm was caused by inappropriate behaviours including bullying, harassment, sexual harassment and victimisation, which resulted in the employee suffering a serious psychological injury.	A breach of sections 19 Primary Duty of Care and 31 Failure to comply with health and safety duty – Category 1 of the WHS Act. The employer faces a maximum penalty of \$3.5 million.
QLD 2024	A construction company was charged and convicted of exposing an employee to a risk of death or serious injury. The employer failed to develop and implement a safe procedure for a task involving unloading steel mesh from shipping containers which required the steel mesh to be removed by a mobile crane. The risk was realised on 8 February 2023 when an employee of the defendant was killed while they used a forklift, slings, and a metal chain to remove steel mesh from a shipping container.	Fine of \$250,000
QLD 2024	An employer was found to have breached its obligation under section 19(1) of the WHS Act, for failing to fulfil its primary duty of care to its workers to ensure their health and safety, so far as is reasonably practicable. It was found that the employer failed to ensure workers received adequate training, resulting in the death of an employee.	Agency was convicted and fined \$425,000

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

VIC 2023	A Victorian Government Department was found guilty of failing to adequately identify and assess risks to employee psychological wellbeing, including exposure to traumatic materials, role conflict, high workloads and work demands, poor workplace relationships and inappropriate workplace behaviours, contributing to a toxic workplace culture and the suicide of an employee.	Department convicted of failing to provide and maintain a safe workplace, resulting in a fine of \$380,000.
NSW 2021	Employee suffered a psychological injury at work following a fatality which the worker witnessed and was initially unfairly blamed for the fatality during the employer's internal investigation. The injuries sustained by the worker were accepted as having left the employee with at least 15% whole person impairment.	Worker's compensation claim resulting in approx. \$1 million award for the injured worker.
QLD 2020	Company found failing to implement control measures that effectively separated mobile plant and pedestrian workers and failing to effectively supervise operators of moving plant and workers resulting in the death of a worker who was crushed by a forklift.	Company fined \$3 million for breach of health and safety duties under the WHS Act.
SA 2015	Truck company owner systematically ignored due diligence obligations, near miss reports, safety issues raised by its workers and failed to exercise due diligence or pay any heed to WHS legislation to repair faulty brakes which led to the death of one of its drivers.	Company owner found guilty of manslaughter and endangering life sentenced to 12 years imprisonment.
TAS 2022	Engineered stone benchtop manufacturer failed to comply with health and safety duties that resulted in workers being exposed to the risk of developing the incurable lung disease silicosis.	Company found guilty to health and safety breaches fined \$500,000.
VIC 2021	Civil construction company failed to provide a safe working environment and provide necessary supervision resulting in two workers being fatally injured when a trench collapsed.	Company found guilty of health and safety breaches fined \$550,000.
WA 2021	Two workers were installing roof sheets on a large machinery shed they were building on a farm without safety control measures in place. Neither of the workers were licensed for the work they were performing, and the worker who was killed did not hold a construction induction training certificate.	Company Director was sentenced to two years and two months' imprisonment (18 months suspended) and fined \$2,250 for gross negligence causing death of a worker and serious injury of another. Company was also fined \$605,000.
NT 2019	Company director fined after an unsupervised apprentice electrician was electrocuted at work.	Company Director fined \$160,000 in the Alice Springs Local Court. The company was convicted and fined \$80,000 for failing to comply with its health and safety duties under the WHS Act and the Company director was convicted and fined \$40,000. The court also ordered the company to provide \$40,000 to NT WorkSafe as an enforceable undertaking to develop an electrical safety campaign.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

PERFORMANCE MANAGEMENT

Lost time injury (LTI) rates have become the cornerstone of mainstream injury/incident reporting and the benchmark against which organisational, industry and national comparisons are made. Although LTI rates are being applied to inform an ever-growing range of health and safety problems and decisions, they also have a number of important limitations, such as a poor correlation with both the human and financial consequences of work related injury and illness.³ There are also considerable variations in the definition of 'lost time' across organisations, thereby making performance benchmarking comparisons difficult.

'Lagging' indicators such as LTI measure outcomes, may not provide sufficient information for successful management, nor provide appropriate information for due diligence purposes. For example, lagging indicators may provide information too late for management to respond.

In contrast, 'leading performance indicators' (LPIs), provide valuable information that helps the organisation respond to changing circumstances and take action to achieve desired outcomes, or avoid unwanted circumstances. Examples of LPIs include:

- the number of hazards reported
- the number of workplace inspections or audits carried out
- the number of actions completed as a result of the inspections/audits performed.

LPIs can play an important role in motivating continuous improvement, with a focus on areas that have the potential to cause an incident, before the incident itself is realised.

WHAT HEALTH, SAFETY AND WELLBEING INFORMATION SHOULD BE PROVIDED TO THE BOARD?

Directors should ensure the appropriate level of information is being reported by management to the board. Reports should be inclusive of lead and lag indicators, and have sufficient information to support the board's decision-making with respect to oversight of health and safety risk. The individual importance of health and safety for directors and the organisation's workforce means that health and safety data should be supported by independent and objective assurance – bringing a systematic, disciplined approach to health and safety risk management, control and governance processes.

For LPIs to be successful they need to be selected carefully; for example, targeting relevant and material issues and setting sufficient challenge. Setting an LPI and obtaining a 'good score' does not automatically improve performance. It is not only the numbers that are important, but the quality and application of the gathered information and the preventative measures put in place that make the difference.

³ Safe Work Australia, updated October 2020, Issues in the Measurement and Reporting of Work Health and Safety.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- Safe Work Australia, <https://www.safeworkaustralia.gov.au/>
- Australian Government Comcare, <https://www.comcare.gov.au/>
- Issues in the Measurement and Reporting of Work Health and Safety: A Review, Safe Work Australia, November 2013.
- Guidance for Officers in exercising Due Diligence, Australian Government Comcare
- Safe Work Australia Australian Work Health and Safety Strategy 2012-2022
- Australian Work Health and Safety Strategy 2023-2033 | Safe Work Australia <https://www.safeworkaustralia.gov.au/doc/australian-work-health-and-safety-strategy-2023-2033>
- Directors' due diligence obligations, Australian Institute of Company Directors, 2025 www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/organisation/governing-whs-psychosocial-risks-web.pdf

For further information please contact:



Paul Rubotham

**Director, Health & Safety,
Audit and Assurance
KPMG Australia
prubotham@kpmg.com.au**

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

22. Culture and Conduct

Boards are accountable for driving an organisation's culture by setting its values and a code of conduct underpinned by processes to ensure all employees demonstrate ethical behaviours to foster a culture of transparency and accountability.

In this chapter

- Tone from the top
- Business ethics
- Organisational values and ethics
- Code of conduct
- Cultural issues
- Developing a 'learning culture' where 'bad news' is communicated
- Whistleblower policy
- Boardroom dynamics
- Information communications outside board meetings

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Are the company's policies and procedures supporting the realisation of the desired culture?
2. Are the code of conduct and compliance program regularly reviewed to determine if they need updating due to business, legal, or regulatory changes?
3. Has the organisation's ethics and compliance program been reviewed by outside consultants or experts for possible improvement?
4. Have any compliance investigations arisen from a cultural problem?
5. Is there a current whistleblowing policy and program in place? How do you know that it is effective?
6. How do individuals receive the information required to understand the firm's core values, code of conduct and the specific policies, laws and regulations related to their jobs?
7. Has a corporate culture been developed and maintained that creates an environment of openness, honesty and the timely reporting of bad news?
8. How does management fully inform the board about potential or actual conflicts between the company's values and the business practices in countries where it operates?
9. What processes and practices are in place to promote ethical behaviour?
10. Does the company have in place processes to monitor and measure culture?
11. Does the board have access to data to assess whether the desired culture of the company is being realised?
12. Has the board considered how executive compensation aligns with the desired ethics and compliance culture?
13. What do the company's internal and external auditors' reports indicate about the organisation's culture? Has the board set an appropriate 'tone from the top'?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The board has 'power factions' that inhibit teamwork.
- The board always comes to a consensus quickly and easily with little or no discussion.
- The code of conduct has not been reviewed in recent years.
- There are a concerning number of internal and external complaints.
- The board receives limited reports or information regarding whistleblower policy.
- The board virtually 'ticks the box' with respect to recommendations from management.
- The board culture does not allow discussion of difficult, controversial or sensitive matters in the boardroom.
- Risk monitoring is not conducted with regards to doing business in higher risk countries.
- The board does not ask questions related to culture, ethics or conduct.
- The board and/or management are not respectful in discussions and reporting on matters involving the regulator(s).
- The importance of culture is not communicated or actively demonstrated by the board.
- Management is rewarded for what they have achieved with little consideration given to how this has been achieved.
- The organisation relies on third parties such as regulators and customers to identify unacceptable business practices or issues.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

While the conduct of financial institutions at home and abroad has garnered considerable attention, a number of other industries have also had their fair share of poor press. Questionable practices in the construction sector, utilities and banking, as well as large retailers and their suppliers, have rocked the public's confidence time and again and led people to question the moral integrity of these organisations. Governmental bodies and agencies are similarly positioned. Concerns around bullying and harassment and a perceived lack of inclusiveness are giving these entities good reason to reconsider their own cultures.¹

It is not surprising then that leading organisations have begun to reflect on the culture and subcultures of their organisations. They are intent on assessing whether issues exist, their underlying causes and what actions could be taken to either change or enrich their organisational culture.

However, it is also important to note that culture cannot be considered in isolation of a number of other tangible organisational initiatives. In particular, remuneration and incentives (decisions about remuneration and incentive structures have a direct influence on both leaders' and staff behaviour), accountability (clearly defined accountability with consequences for poor risk and customer outcomes drives the required message from management), governance, and, most importantly, leadership ('tone from the top').

TONE FROM THE TOP

Whilst many organisations implement policies and frameworks that outline the conduct and behaviours expected of individuals, they are often initiated in response to legal requirements and other guidelines. Although it is important that an ethics and compliance program is in place, it must be more than just adherence to rules and policies. Instead, an ethical culture should be embedded into an organisation. Merely meeting legal requirements is unlikely to be sufficient to satisfy the ethical concerns of employees, clients, customers, shareholders and other stakeholders.

¹ Refer to KPMG, Risk Consulting: Organisation's cultural assessment and transformation, <https://assets.kpmg/content/dam/kpmg/ie/pdf/2017/07/ie-risk-cultural-assessment-transformation.pdf>

The commitment of the entire organisation is essential in order to design, develop and implement an effective corporate culture. It represents 'how we do things around here' and sets the basis of acceptable behaviours and cultural norms. Having policies in place is a start, but the real test of an organisation's culture is what happens in practice. There is often a marked difference between what is written in policy and how things are done in practice. Boards set the 'tone from the top', which influences the entire organisation. The board should ensure appropriate values, ethics and culture are upheld throughout the organisation.

Increasingly, there have been many examples of where organisational behaviour has been at odds with stated policies. In some instances it has been individual 'bad apples' that have 'spoiled' the entire organisation through discrete acts of unethical behaviour. However, more often, the issues are more systemic, where unethical conduct has represented a culture of complicity or risk-taking that is at odds with the stated policies. Research has shown that ethical culture is often based on the behaviour of peers² and immediate managers.³ Setting the right 'tone from the top' is therefore an important factor in shaping the ethical and behavioural standards that the organisation is willing to accept, including holding staff to account when these standards are not met – regardless of whether the poor conduct is reported publicly or not.

The 'tone from the top' refers to the character and behaviour displayed by leaders of an organisation that forms a model of appropriate conduct for every level of the organisation. Boards bear ultimate responsibility for their organisation's culture, including the values and ethical environment that underpin that culture. The 'tone from the top' should be underpinned by clearly articulated values and policies, a code of conduct, ongoing ethical awareness training and an ethics management process that is embedded across all the organisation's activities.

² Collins, F. (2006). Career Self-Interest and Concern for Others – The Effects of Co-Worker Attitudes on Fraudulent Behavior. *Accounting & The Public Interest*, 695-115.

³ Schaubroeck, J. M., Hannah, S. T., Avolio, B. J., Kozlowski, S. W., Lord, R. G., Treviño, L. K., & Peng, A. C. (2012). Embedding Ethical Leadership Within And Across Organization Levels. *Academy Of Management Journal*, 55(5), 1053-1078. doi:10.5465/amj.2011.0064

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

It is also important to note that the dissemination and reinforcement of desired conduct and values is also important as, without an 'echo from the bottom' or staff engagement, the 'tone from the top' is of limited utility.⁴



Case study: lessons in culture from the Financial Services Royal Commission

Changing culture and governance was a centrepiece of the Hayne Royal Commission's Final Report. Commissioner Hayne directed that financial services entities are to take proper steps to assess the entities' culture and governance, identify any problems, deal with those problems and thereafter determine whether the changes made have been effective.

For many organisations, conducting a risk assessment and outlining remedial actions are already part of their ongoing activities. However, risk culture is a nebulous concept, and difficult to measure in any quantitative way outside of one-dimensional risk surveys. Demonstrating genuine effectiveness of cultural change will be a challenge for many. Measuring the effectiveness of changes is made more challenging as organisational culture is built over time and is only changed slowly.

APRA has been directed to re-establish their culture supervisory capabilities, and to take a more active role in the supervision of culture including 'assessing the cultural drivers of misconduct in entities'. Organisations wanting to avoid close cultural scrutiny from APRA would do well to take steps to understand and deal with their cultural problems as the recommendation suggests a 'risk-based approach' given that cultural work can be resource-intensive and therefore focused.

Culture is also addressed in the 4th edition of the ASX Corporate Governance Principles, with principles and recommendations that focus on the link between culture, values and community expectations. The 4th edition includes significant changes to Principle 3, with an overarching view that it is imperative that listed entities align their culture and values with community expectations, to help address a declining trust in business so as to build long-term sustainable value for their security holders.⁵

Specifically, Principle 3 provides that 'a listed entity should instil and continually reinforce a culture across the organisation of acting lawfully, ethically and responsibly'.⁶ This is consistent with the themes that emerged from the Financial Services Royal Commission noted above.

The specific recommendations under Principle 3 include having and disclosing:

- the entity's values
- a code of conduct
- a whistleblower policy
- an anti-bribery and corruption policy.

⁴ Group of Thirty, 'Banking Conduct and Culture: A Call for Sustained and Comprehensive Reform' (July 2015) at 13.

⁵ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, Principle 3. 2019.

⁶ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, Principle 3. 2019. P 16.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

It appears from the consultation draft for a proposed fifth edition of the Corporate Governance Principles⁷ that in the next iteration Principle 3 will extend further to be explicit regarding how this culture extends to 'dealings with external stakeholders, to create long-term sustainable value'. In particular the consultation draft included the following:

Indicators of a healthy organisational culture include:

- a 'speak up culture' which promotes listening to staff and respectful treatment of internal and third-party whistleblowers
- appropriate escalation of issues from management to the board, or a board committee, including information on patterns of behaviour which may be material when taken as a whole
- a culture which recognises and has regard to the interests of internal and external stakeholders, to create long-term sustainable value
- a risk culture which supports early reporting and timely remediation of risk, with learning outcomes.

For example, material breaches of the code of conduct, whistleblowing incidents and breaches of the entity's anti-bribery and corruption policy should be promptly reported to the board, or a board committee. Where reporting is to a board committee, there should be escalation of issues to the board, where appropriate.

The entity's code of conduct should support the lawful, ethical and responsible operations of the entity, in the best interests of the entity (including having regard to the interests of the entity's key stakeholders).

Notwithstanding that the ASX have indicated that this consultation draft will not proceed to a fifth edition, this commentary from them is worth noting.⁸

⁷ ASX, Consultation Draft for a proposed fifth edition of the Principles and Recommendations, <https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/corporate-governance-principles-and-recommendations-consultation-draft.pdf>

⁸ ASX, Consultation Draft for a proposed fifth edition of the Principles and Recommendations, <https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/corporate-governance-principles-and-recommendations-consultation-draft.pdf>

BUSINESS ETHICS

Business ethics refers to rules, standards, stated organisational values and behaviours that determine what is acceptable or unacceptable in specific situations. They are inextricably linked to notions of honesty, integrity, trust, accountability, transparency and social responsibility. Ethical conduct is a key factor in the long-term viability and success of organisations. Moreover, the reputations of individual directors and executives are tarnished when a business is seen not to have acted ethically, or has otherwise breached community standards.

An organisation's business ethics and corporate culture may be revisited in conjunction with a board review or a review of the organisation's remuneration practices. Perceived failures, adverse media exposure and episodes of high staff turnover are examples of possible catalysts for a reawakening interest in business ethics and corporate culture; a tool to revitalise the organisation.

An effective business ethics process should generate real benefits, including:

- increasing the integrity of financial reports and information
- minimising the incidence and encouraging the reporting of fraud and other organisational misconduct
- creating confidence that unethical behaviour will be reported and addressed
- producing a working environment that fosters pride, responsibility and a sense of both purpose and value.

The following is an example of a business ethics framework.

- A code of conduct that clearly and concisely articulates an organisation's values and behaviours.
- A code of conduct which underpins all organisational activities, sets out the organisation's employment practices, and provides direction on how management will manage the business.
- Ethics and awareness training should be delivered and reinforced regularly to all employees, and included in induction programs for new employees.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

- Formal processes providing guidance to employees facing ethical dilemmas, and the mechanisms for reporting wrongdoing, and making suggestions about how business ethics can be improved.
- A performance management process that not only measures results, but considers how these results have been achieved.

TRENDS

Moving away from 'can we' to 'should we'

For over a decade, the CBA had been using the word 'can' in its marketing campaigns, however, in April 2018 the prudential regulator, APRA, demanded that the question 'should we' be injected into the bank's culture in relation to all dealings with and decisions on customers.

The Inquiry Panel explored the concept of conduct risk management, which it noted in its simplest form goes beyond what is strictly allowed under law and regulation ('Can we do it?') to consider whether an action is appropriate or ethical ('Should we do it?'). The Panel also noted that compliance functions globally have more recently been focused not just on evaluating with business units whether an activity or product is allowed under regulation ('Can we?') but, critically, whether they should engage in such an activity or product in the first place ('Should we?').

ORGANISATIONAL VALUES AND ETHICS

Organisational values not only guide a company's people, but also create expectations on the part of external stakeholders about acceptable behaviour within the organisation. Strong values shared by both an organisation and its employees have been found to increase employee commitment and satisfaction. This in turn is said to lead to a strong culture.⁹

9 Adamoniene R. et al, June 2021, Influence of individual and organisational variables on the perception of organisational values.

Once agreed, values should be embedded in documented policies and procedures, and then actively embraced and practised by all company personnel. An effective ethics and compliance program requires senior management leadership to entrench and uphold values, organisation-wide commitment, an effective communications system and an ongoing monitoring system.

CODE OF CONDUCT

Good corporate governance is ultimately about personal and organisational integrity. Although this cannot be regulated, investor confidence can be enhanced if the company clearly articulates acceptable practices for directors, senior executives and employees.

Typically, a code of conduct:

- spells out an organisation's values and principles
- reflects and shapes the organisation's culture
- makes transparent the value framework within which the organisation operates.

The ASX Corporate Governance Principles recommend that companies establish a code of conduct that articulates the standards of behaviour expected of its directors, senior executives and employees, and ensures that the board or board committee is informed of any breaches.¹⁰

Box 3.2 of the ASX Corporate Governance Principles includes a detailed list of suggested matters which may be useful for consideration when formulating a code of conduct. Codes of conduct should reflect the company's unique operating and contextual environment.

As the board and senior executives are responsible for setting the tone and ethical standards of the organisation and overseeing adherence to them, they must demonstrate that the agreed codes and standards are equally applicable to them and lead by example. Organisations that 'walk the talk' with regard to their code develop a reputation for honesty, integrity and principled business behaviour, which may form a key element of a company's brand and enhance its reputation.¹¹

10 ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, Recommendation 3.2. 2019.

11 20 Questions Directors Should Ask about Codes of Conduct, Gunns, M. & Wexler, M. 2010.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The Governance Institute of Australia recommends that directors be required to commit to the code of conduct on appointment, regularly review the code of conduct, and seek assurance that relevant compliance systems are in place and are operating effectively.¹² When overseeing the implementation of the code, directors must ensure it is effectively communicated by management. The board should make certain that the code of conduct is taken seriously throughout the organisation, and breaches will give rise to disciplinary measures. Merely issuing a code, however, does not ensure it will be observed. To add value, the code must extend beyond a compliance focus and strive to cultivate and maintain an organisation-wide culture that focuses on encouraging positive moral behaviour while simultaneously striving to prevent ethical lapses.¹³

The code of conduct must continue to evolve with the changing environment. This includes laws and regulations, the operational environment, public opinion and the focus on acceptable business behaviour. Those developing or revising the code of conduct should consult frequently with specialists in areas addressed by the code.

CULTURAL ISSUES

Global operations

Companies with significant global operations face additional difficulties in evolving and implementing codes of ethics and conduct. In part, it is a matter of different cultural norms – what is generally acceptable in Australia might not be so acceptable in another country.

The board should be fully informed about conflicts between the company's values and business practices in various countries, as a lack of understanding of cultural differences may contribute to compliance breaches of international laws (e.g. bribery and facilitation, work health and safety practices), a lack of performance, loss of key employees and time-consuming conflicts.

Multinational companies are faced with several issues:

- how to foster a culture of ethical conduct in all countries of operation
- how to navigate cultural differences and norms
- how to ensure suppliers adhere to ethical codes of conduct
- how to engage a global workforce in understanding and adopting its corporate values
- how to meet all the legal and compliance obligations throughout all locations
- language barriers between different global units.

When selecting leadership roles within a multinational company, cultural alignment may be a relevant consideration, in an attempt to promote consensus on a global, organisation-wide culture, particularly when appointing local leaders across international business units. Cultural alignment of potential candidates must therefore form part of any skills and attributes assessment, together with other criteria such as gender, age and ethnicity. When considering cultural alignment, best practice is to clearly define the organisation's culture (e.g. values, processes, expected behaviours, accountability processes and leadership style) and transparently measure candidates against this standard. It cannot be based on a gut feel.

However, it is counterintuitive to require everyone to be the same in an organisation to foster an ethical culture. The key will be to keep ethics on the agenda and through regular communication, keep leaders accountable for ethical conduct to each other and to the board. A better selection tool would be a thorough background check for any history of ethical misconduct.

A failure to consider an organisation-wide code of conduct may lead to significant cultural differences in the executive levels of the company around the world, potentially fostering a lack of understanding and commonality of purpose that may lead to conflict and poorly executed decisions. Global principles, based on corporate values, should be promoted across the organisation, while still allowing for local cultural traditions within international business units.

¹² Governance Institute of Australia, Good Governance Guide – Corporate Code of Conduct, 2011.

¹³ K. M. Gilley, C. Robertson, T.C. Mazur, The bottom-line benefits of ethics code commitment, 2010.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Mergers and acquisitions

A 2020 research paper explains that analysts tend to overestimate revenue gains and cost savings from synergy but underestimate the implementation challenges caused by culture and people.¹⁴ In other words, cultural differences are a major post-deal issue, and companies frequently underestimate issues with cultural variation and complexity. Organisations should pre-empt these issues, as opposed to blaming cultural differences for difficulties experienced during post-deal integration.

Central considerations in managing the integration of company cultures include:

- assessing the differences in cultures from the outset
- defining a cultural end state and its implications for future ways of working
- engaging in deep cultural learning to move towards acculturation
- retention of rewards for key people
- understanding what makes each and the combined business successful, and how this will be retained and built on.¹⁵

It should be considered whether the cultures of the two organisations are compatible, and if one will be dominant, how employees operating under the alternative culture will be embraced. If one culture is to prevail, retaining key leaders of that organisation to serve as role models is essential in order to promote the integrated culture. The key objective in some mergers or acquisitions is to incorporate the advantages of each organisation's culture, ultimately resulting in synergy. The possible end states for a merger or acquisition are found in Figure 1. A plan for the merging of cultures should be devised, depending on the defined cultural end state, incorporating educational efforts to assist employees to understand the corporate values they should adopt in the workplace.

¹⁴ D. Wang, D. S. Hain, J. Larimo, L. T. Dao, *Cultural Differences And Synergy Realization In Cross-Border Acquisitions – The Moderating Effect Of Acquisition Process*, International Business Review, February 2020.

¹⁵ Marks, M. L., & Mirvis, P. H. (2011). A framework for the human resources role in managing culture in mergers and acquisitions. *Human Resource Management*, 50(6), 859-877.

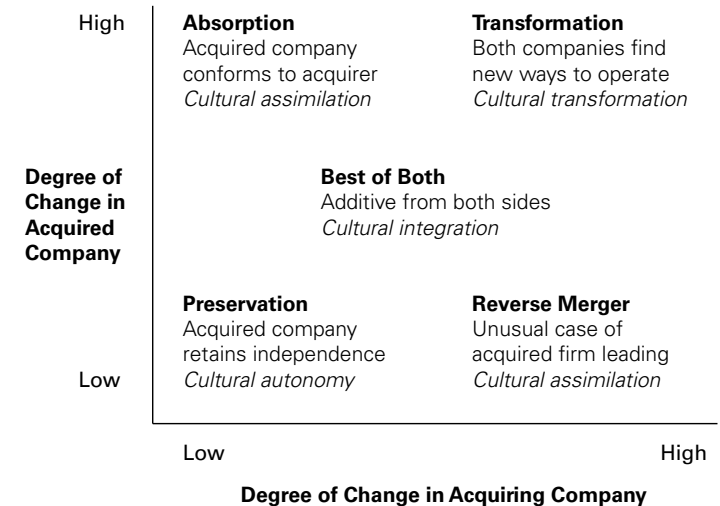


Figure 1. Possible cultural end states resulting from a merger or acquisition.

DEVELOPING A 'LEARNING CULTURE' WHERE 'BAD NEWS' IS COMMUNICATED

Recent corporate scandals highlight the importance of building a corporate culture that supports the giving and receiving of 'bad news', i.e. creating an environment of openness and honesty and the presentation of the hard truth.

A KPMG-sponsored survey found that only 55 percent of respondents believe that their organisation is effective at keeping the board aware of the key risk issues.¹⁶ This is a cultural issue that the board must be cognisant of, ensuring that it builds an environment where 'bad news' can be delivered without fear of retribution or personal repercussions. In practice, this requires boards to question information provided by management and seek any additional information from the organisation that can assist in identifying and managing 'bad news', without creating an environment of 'punishment' of those who raise the issues.

¹⁶ KPMG, 2011, Enhancing Business Performance through Governance, Risk, and Compliance.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

An early warning system for problems can present the opportunity for timely and appropriate intervention, learning and continuous improvement and/or the redefining of strategy. A climate in which full disclosure is delivered in a timely manner should be fostered by senior management and endorsed by the board to encourage employees to immediately bring forth concerns. This relies on the implementation of processes to support accurate and timely reporting, as well as a culture of accountability, trust and openness which can only be built on individual and collective behaviours displayed and accepted by the board.

WHISTLEBLOWER POLICY

The term 'whistleblower' refers to anyone who alerts superiors or the appropriate authorities to misconduct within an organisation (although we note that under the Corporations Act the term 'whistleblower' has a specific meaning and refers to individuals who make disclosures that are protected under the law). All employees and related individuals such as contractors and suppliers should be encouraged to raise genuine concerns about possible improprieties in the conduct of an organisation's business.

Employees may fear retribution or retaliation if they take their concerns to management or believe their allegations will not be taken seriously. They might not know who they should take the matter up with, and this becomes a more acute concern when the subject of the allegation is their manager or someone more senior.

Many companies use external reporting services to allow for anonymous reporting and eliminate the fear of retaliation. These services usually provide staff with a toll-free telephone number or web-based report for reporting their concerns about fraudulent or improper conduct. All whistleblower reports should be assessed internally. If they appear to be genuine (i.e. there are reasonable grounds to suspect misconduct or an improper state of affairs) they should be investigated, where possible, and reported (using anonymised information) to the relevant committee. Some companies appoint a whistleblower officer for this purpose.

Recommendation 3.3 of the ASX Corporate Governance Principles and Recommendations provides that a whistleblower policy should identify the types of concerns that may be reported under the policy, explain how the confidentiality of the whistleblower will be safeguarded and how they will be protected from victimisation, and provide training on employee rights and managerial responsibilities under the whistleblower policy.¹⁷ A robust whistleblowing policy that is supported and implemented by an effective whistleblowing program will be particularly critical for companies given the changes to whistleblower protections laws.

From 1 July 2019, the whistleblower protections of the Corporations Act were expanded to provide greater protection for 'eligible whistleblowers', which includes current and former officers, employees, contractors and suppliers of a company, as well as their spouses, immediate family and dependents, who report information that they have 'reasonable grounds to suspect' indicates misconduct or an improper state of affairs in relation to the company.¹⁸ Whistleblowers must make their disclosures to 'eligible recipients' in order to access the protections. Eligible recipients include directors, company secretaries or senior managers of the company or organisation as well as members of the audit team and a person or service designated by the company to receive disclosures (refer to further changes to whistleblower protection laws below).

¹⁷ ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, 2019, Box 3.3.

¹⁸ Corporations Act 2001, Part 9.4AAA.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Changes to whistleblower protection laws

In February 2019, the Federal Government passed a bill to strengthen Australia's [whistleblower protection laws](#). The laws are the first major update of Australia's whistleblowing protections in nearly two decades, and impact almost every Australian business. The bill has amended both the corporate and taxation laws to put in place a comprehensive series of safeguards for those individuals who disclose corporate or taxpayer misconduct. The updated protections include:

- the ability for whistleblowers to make anonymous disclosures, and have their identity protected (including fines for revealing a whistleblower's identity without consent)
- an increased pool of potential whistleblowers will be eligible for protection (including former employees)
- a wide scope of disclosable matters, including information concerning 'misconduct or an improper state of affairs'
- the ability for whistleblowers to disclose the information to a Member of Parliament or a journalist if no action is taken in response to a disclosure to a regulatory body
- mandatory whistleblower policies for public companies, large proprietary companies and proprietary companies that are trustees of registrable superannuation entities.

BOARDROOM DYNAMICS

Board culture underpins board dynamics and has a decisive influence on performance. A well-functioning board generally displays coherence, trust and common values between members, encourages and has regard to differing viewpoints and opinions, and is able to reach a decision without animosity.¹⁹ Healthy boardroom dynamics will encourage sound decision-making that delivers value to shareholders.

The working relationship between directors and management is one of the most influential factors in board effectiveness. Most productive relationships are built on mutual trust and respect, where both the board (and the chairman in particular) and the CEO work in partnership, each with an acute appreciation of the vital role played by each other in building shareholder value. Dysfunction can occur where either the chairman or the CEO is overly controlling and this behaviour goes unchecked.

INFORMAL COMMUNICATIONS OUTSIDE BOARD MEETINGS

Informal communication is one of the most effective ways of sharing information, building knowledge and fostering constructive working relationships. For this reason, boards that communicate regularly, when necessary, with each other and management, are typically strong decision-makers.

¹⁹ Australian Government: Corporations and Markets Advisory Committee: Diversity on Boards of Directors, March 2009.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

TRENDS

Utilising independent measurement to understand culture

Internal audit and other external service providers also have a critical role to play in understanding and reporting on the human factors that impact on the processes, risks and controls in an organisation. As part of internal audits, organisations are now receiving reports on the cultural aspects of the internal audit engagements undertaken using a mixture of auditing techniques such as interviews, observations, surveys, data and documents analysis.

KPMG Internal Audit for example, can help to improve the internal audit quality by incorporating behavioural controls into a company's internal audit approach and reporting on behavioural controls findings and recommendations. We do this by using a mixture of auditing techniques noted above, as well as utilising a mixture of experts having a diverse educational background, for example psychology, sociology and business studies. Our internal audit reports are fact-based, specific and future-oriented.

Learn more about KPMG's [model](#) for understanding cultural drivers or read our factsheet: [Behavioural drivers in Risk, Compliance & Assurance](#)

Incentive systems

Remuneration is also a key driver of culture, thus, having the right incentive systems is another important consideration for the board.²⁰ This includes the recruitment, performance management, remuneration and promotion systems that should not only reward good business performance but also take into account adherence (and non-adherence) to the company's culture and behavioural standards. This should avoid incentivising short-term business performance at the expense of the interests of stakeholders and the safety and soundness of the organisation. Companies should also establish clear and appropriate consequences, articulated and applied for staff found to be engaging in any undesirable or unacceptable behaviours.

Commentary in the ASX Corporate Governance Principles and Recommendations makes clear that when determining appropriate remuneration structures, consideration should not only be given to incentivising executives and directors to pursue the growth and success of the organisation, but also to the need to ensure that incentives do not reward 'conduct that is contrary to the entity's values or risk appetite'.²¹ In addition, consideration should be given to the implications of being perceived by the community to be paying excessively.²²

20 Commissioner Hayne in the Interim Report, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry 28 September 2018, Volume 1, at page 5.

21 ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, Recommendation 8.1. 2019.

22 ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, Recommendation 8.1. 2019.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- ASIC Regulatory Guide 73, *Continuous Disclosure Obligations: Infringement Notices*, Reissued 31 October 2017, <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-73-continuous-disclosure-obligations-infringement-notices/>
- APRA Risk Culture Information Paper, October 2016, <https://www.apra.gov.au/sites/default/files/161018-information-paper-risk-culture1.pdf>
- Australian Prudential Regulation Authority, *Prudential Inquiry into the Commonwealth Bank of Australia*, 30 April 2018. Available at https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf
- Australasian Investor Relations Association website, <https://www.australasianir.com.au/>
- IIRC Discussion Paper, *Towards Integrated Reporting – Communicating Value in the 21st Century*, September 2011, https://www.integratedreporting.org/wp-content/uploads/2011/09/IR-Discussion-Paper-2011_spreads.pdf
- APRA Insight, *Transforming risk culture*, 14 October 2021, www.apra.gov.au/news-and-publications/apra-insight-transforming-risk-culture
- KPMG, Unlocking the upside of conduct risk, <https://home.kpmg/au/en/home/topics/conduct.html>

For further information please contact:



Dr Meg Brodie
Partner in Charge, ESG Social
KPMG Australia
megbrodie@kpmg.com.au



Jacinta Munro
Partner, Risk Assurance
KPMG Australia
jacintamunro@kpmg.com.au

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

23. Cybersecurity

Cybersecurity continues to be a strategic risk for all organisations and a topic for discussion at board-level with major incidents increasingly commonplace across a range of industries.

In this chapter

- Introduction
- The rise of ransomware
- Regulatory changes in response to cybersecurity risks
- Cyber risk management
- What should a board consider?
- Cyber strategy aligns with business strategy
- Roles and responsibilities for cybersecurity have been defined and communicated
- The security model is comprehensive
- Security and privacy aligned
- Cybersecurity and data privacy in business continuity plans
- Critical success factors

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. How does the Board maintain awareness of the cybersecurity threats and risks and how they affect the organisation? Has the Board agreed their cyber risk appetite for the company? Does the Board understand the key cybersecurity risks that have been accepted by the executives and whether this is within the board's stated cyber risk appetite?
2. Is cybersecurity discussed at Board-level? If so, what key risk indicators are considered and how does the board support effective risk management in this area?
3. Does the Board have the right cyber expertise to fulfill its accountabilities?
4. Are the Board confident that the organisation will know if it has been breached? What makes the Board certain that it will find out in the right time frame? Does the Board know how to respond to a cyber incident, including its role and the roles of other response teams (e.g., the Crisis Management Team, Legal, Communications, Business Continuity etc.)?
5. Does management have a ransomware response plan? Do we have a board-approved policy on ransom payments?
6. Are cybersecurity aspects considered in major business decisions, such as mergers and acquisitions, partnerships, new product launches?
7. Does the organisation have a cybersecurity programme to meet the challenges of today's (and tomorrow's) cyber threat landscape?
8. Is there an ongoing, organisation-wide awareness and training program established around cybersecurity?
9. How quickly can the organisation restore its critical processes and systems after they have been taken out in case of a large-scale cyber-attack? And how long can the company survive without its critical processes and systems?
10. What are the organisation's key regulatory obligations for cyber? Does it have a calendar of obligations? Does it have a defined process to report these, with adequate oversight and counterbalance?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- Cybersecurity is not a routine topic discussed by the Board or sub-committee agenda.
- Cyber risk is not specifically included in assessing business and operational risk.
- Cyber risk appetite has not been set, and the organisation does not know how much it is spending on cybersecurity and whether this is enough.
- Specific accountability for cyber risk management / treatment, planning, and reporting is not defined.
- Organisational strategy and planning do not consider cybersecurity in the ever changing digital landscape.
- Cyber incident response simulations have not been conducted across all levels, from executives, management and Board members, to operational response teams.
- Management has not tested in the last year whether critical processes and systems can be recovered in adequate time after being taken out after a cyber incident.
- The Board has not set a cybersecurity strategy or approved any security policies.
- Cyber controls are not consistently applied across the organisation and thus it may potentially be in breach of our key regulatory obligations.
- The Board not being timely informed in case of material cybersecurity breaches.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

INTRODUCTION

Board level awareness and decision making regarding current and emerging cyber risks is critical for the ongoing cyber resilience of an organisation. It is important that Directors are proactive and focused on mitigating cyber risk; Boards have woken up to the call that they must address cybersecurity issues on their front lines, and that it is not just an IT issue. Cyber risks are an enterprise-wide risk management issue that could impact the entire business as well as its suppliers, partners and customers.

Senior leaders now understand that getting cybersecurity right and managing the risk effectively can create a strategic advantage. However, to achieve long term success, strategic decision-making and the management of cyber risk must start from the top down.

Cyber criminals are well organised, resourceful and well-motivated. Hence, organisations must employ highly skilled cybersecurity experts to address the constantly evolving threats from cyber criminals.

For a number of years now, Boards have required cybersecurity to become a top investment priority. However, KPMG's experience is that although there is some fatigue around the issue, there is still a cybersecurity knowledge gap amongst some Boards. Specifically, smaller and medium sized organisations typically still have a skills gap when compared with the major organisations.

THE EVOLUTION OF CYBER ATTACKS

Cyber-attacks are continually evolving, with attackers constantly changing their tactics to overcome modern security solutions, controls, and processes. As technology advances, so do the methods used by cyber criminals to exploit vulnerabilities and gain unauthorised access to systems and data. Organisations must stay vigilant and adapt their security measures to keep up with these evolving threats. This requires a proactive approach to monitoring and responding to new attack techniques, as well as ongoing education and training for employees to recognise and prevent potential cyber incidents.

One of the most common types of cyber-attacks today is phishing. Phishing involves sending fraudulent emails or messages that appear to be from legitimate sources, with the goal of tricking individuals into revealing sensitive information or clicking on malicious links. These attacks can lead to the installation of malware or the theft of personal data, such as passwords and credit card numbers. Phishing remains a prevalent threat due to its simplicity and effectiveness in targeting unsuspecting users.

Another widespread cyber-attack technique is malware. Malware encompasses various types of malicious software, including viruses, worms, trojans, and ransomware. These programs can infiltrate systems, steal data, disrupt operations, or demand ransom payments. Malware can be delivered through email attachments, infected websites, or software downloads. Once installed, malware can spread rapidly and cause significant damage to an organization's network and data.

Denial-of-Service (DoS) attacks are also common in modern cyber incidents. DoS attacks aim to overwhelm a system, network, or website with excessive traffic, rendering it unavailable to users. Attackers use various methods, such as flooding the target with requests or exploiting vulnerabilities, to disrupt normal operations. Distributed Denial-of-Service (DDoS) attacks involve multiple compromised devices working together to amplify the impact. These attacks can result in downtime, loss of revenue, and reputational damage.

Man-in-the-Middle (MitM) attacks occur when an attacker intercepts and alters communication between two parties without their knowledge. This can happen in various ways, such as through compromised Wi-Fi networks or malicious software. The attacker can eavesdrop on conversations, steal sensitive information, or inject malicious content into the communication. MitM attacks pose a significant threat to the confidentiality and integrity of data exchanged between users.

Lastly, SQL injection is a technique where attackers exploit vulnerabilities in web applications to execute malicious SQL queries. By inserting malicious code into input fields, attackers can gain unauthorized access to databases, retrieve sensitive information, modify data, or even delete records. SQL injection attacks can have severe consequences, including data breaches and loss of critical information.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

LEGISLATIVE CHANGES IN RESPONSE TO CYBERSECURITY RISKS IN AUSTRALIA

Recent changes to cyber legislation and regulation in Australia have been significant, aiming to enhance the country's cybersecurity posture and align with international best practices. These changes were introduced through the Cybersecurity Legislative Package, which includes the Cybersecurity Act 2024, the Intelligence Services and Other Legislation Amendment (Cybersecurity) Act 2024, and the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 (ERP Act).

- The Cybersecurity Act 2024 was introduced to address legislative gaps and ensure that Australia is on track to become a global leader in cybersecurity. This act clarifies existing obligations for critical infrastructure owners and operators to protect data storage systems that hold business-critical data. It also introduces new powers for the Minister for Home Affairs to issue directions to address the impacts of all-hazards incidents on critical infrastructure. These changes are designed to enhance the protection of critical infrastructure and improve the country's ability to respond to cyber threats.
- The Intelligence Services and Other Legislation Amendment (Cybersecurity) Act 2024 establishes a new definition of 'protected information' as confidential commercial information or information that, if disclosed, could harm the public, the security of a critical infrastructure asset, or Australia's national security. This act also introduces a power for the regulator to issue formal written directions to address seriously deficient elements of any risk management program. These changes aim to strengthen the protection of sensitive information and ensure that organizations have robust risk management practices in place.
- The ERP Act includes several schedules that address various aspects of cybersecurity. Schedule 1 clarifies existing obligations under the Security of Critical Infrastructure Act 2018 (SOCI Act) for critical infrastructure owners and operators to protect certain data storage systems. Schedule 2 allows the Minister for Home Affairs to authorize the Secretary of Home Affairs to issue action

and information gathering directions to address the impacts of all-hazards incidents on critical infrastructure. Schedule 3 establishes a new definition of 'protected information'. Schedule 4 introduces a power for the regulator to issue formal written directions to address seriously deficient elements of any risk management program. Schedule 5 enhances telecommunications security obligations for critical telecommunications assets. Schedule 6 removes the requirement for the Minister for Home Affairs to notify each direct interest holder for a critical infrastructure asset declared to be a System of National Significance (SoNS) and only requires the responsible entity to be notified.

These legislative changes affect a wide range of stakeholders, including critical infrastructure owners and operators, telecommunications providers, and organizations that handle sensitive information. The changes have been brought in to address the evolving cyber threat landscape, enhance the protection of critical infrastructure, and ensure that Australia remains resilient against cyber-attacks.

CYBER RISK MANAGEMENT

To effectively manage cybersecurity risks (as portrayed in the image below), an organisation's people, processes and technology must work in partnership towards the same objectives. Cyber risk management is a fundamental component of governance and must be integrated with supporting activities enterprise wide. This cannot be left solely to the technical specialists in IT and cannot be addressed in isolation. It is important that the Chief Information Security Officer (CISO), or equivalent, is an effective communicator to be able to work with the board to embed cybersecurity into an organisation's operating model.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

It is critical that boards continue to drive a robust approach to managing cyber risk to reduce volatility and uncertainty. A robust cybersecurity assessment should focus on 'cybersecurity leadership, governance, people risks, legal and regulatory compliance, business continuity plans, the organisation's operating model, technology and information risks'. All organisations should periodically review their cybersecurity risk assessments to prevent, detect, contain and respond to threats to their critical processes and systems.



Source: KPMG

WHAT SHOULD A BOARD CONSIDER?

Boards are increasingly getting to grips with the risks that cyber threats pose to their business, both strategically and operationally. KPMG's experience is that boards frequently raise the need for more cybersecurity skills and experience in the boardroom. Despite this, we note that many boards do not have a clear understanding what their cyber risk appetite is and whether the company is spending enough money on cybersecurity and in the right areas.

Boards with the support of their sub-committees should continue to evaluate and coordinate the delegation of oversight for cybersecurity. KPMG's experience is that many audit committees continue to oversee cybersecurity and data privacy. However, as cyber risks becoming increasingly complex, it is important boards consider whether these risks require more attention at board-level or potentially in a sub-committee dedicated to IT, cyber and data governance. The addition of a sub-committee depends on the size and nature of the organisation as well as whether there is the right mix of skills and experience on the board, and sub-committees, to have robust conversations with management on cyber risks, and whether the organisation is doing enough.

Regardless of how the board and sub-committees are structured, the board should frequently obtain cybersecurity scorecards from management and continue to challenge the company's ever-changing cyber risk profile, the effectiveness of its control environment, and its readiness to timely respond to and recover from cyber attacks. This will improve reporting and discussions at board-level about cybersecurity.

While board members are aware of the personal cyber risks they face alongside the corporate threat, it is important that they have a full understanding of the dangers as these evolve. Directors who have received no cyber risk training and participated in a cyberattack simulation over the past 12 months should be encouraged to sign up for support in the year ahead.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

CYBER STRATEGY ALIGNS WITH BUSINESS STRATEGY

Cybersecurity must be an enabler to the overarching business strategy and must consider what the business wants to achieve and by when. Security cannot be so restrictive that it hinders innovation and service delivery, and it must be proportionate to the risk(s) that the business faces. A good cybersecurity strategy will have clear linkages to an organisation's vision, objectives and innovation projects and businesses will have determined appropriate levels of acceptable risk.

Too often efforts to manage cyber related risks are not coherent with the overall business strategy. Many organisations fail to ask themselves: 'What are we trying to achieve as a business, and what are the cyber threats to those objectives that we need to counter?'

Cyber risk is an important strategic concern for boards of directors. Its true nature is dependent upon external threat factors, as well as the industry sector, business activities and corporate objectives.

A clear linkage between business objectives, the threats to those objectives, risk appetite and the enabling security capabilities to counter the threats, makes the investment decision easier and it becomes a more straightforward balance between Return on Investment (ROI) and residual risk.

Without a clear strategy and roadmap, people look for the latest, greatest thing being promoted in the market. Organisations end up focusing disproportionate resources into the implementation of expensive technology solutions – viewing them as some kind of universal panacea for any security fears – rather than emphasising skills and awareness or focusing on targeted security investments to enable business change.

ROLES AND RESPONSIBILITIES FOR CYBERSECURITY HAVE BEEN DEFINED AND COMMUNICATED

Making it clear who is accountable for any type of risk or action is a crucial element of good governance. Organisations may assign senior responsibility for cyber risks to the Chief Financial Officer (CFO), the Chief Executive Officer (CEO), the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO). Clear cut accountability is essential for effective cyber risk management but remember that final accountability always remains with the board.

People are crucial to the successful implementation of behaviours and controls that protect information and assets. A well thought-out, routine and up to date programme for training and awareness activities that covers employment from onboarding to termination is critical to preventing cyber-attacks and data breaches.

Reality shows that cybersecurity is very much driven by compliance. This is understandable, because many organisations have to accommodate a range of laws and legislation. However, it is counterproductive to view compliance as the ultimate goal of cybersecurity policy. Only an organisation that is capable of understanding external developments and incident trends, and using this insight to inform strategy and policy, will be successful in combating cyber-crime in the long term. Hence, it is important that all roles and responsibilities are communicated across the whole of the organisation and all employees receive regular cyber training. Regular training will allow all staff to understand and look out for the risks and threats that can impact their day-to-day activities.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

THE SECURITY MODEL IS COMPREHENSIVE

Controls and processes must cover all areas of cybersecurity and be designed and implemented to manage specific risks. There are various security models that organisations can use to align and map cyber practices against recognised industry standards. These frameworks include the Australian Signals Directorate Essential Eight Strategies for Mitigating Cyber Incidents (the ASD E8). It was released in 2017 and the ASD has been updating it regularly. It provides baseline mitigation strategies which are intended to make 'it much harder for adversaries to compromise systems'. These are as follows and a maturity model is available to understand the level of maturity against each strategy:

1. Application control
2. Patch applications
3. Configure Microsoft Office macro settings
4. User application hardening
5. Restrict administrative privileges
6. Patch operating systems
7. Multi-factor authentication
8. Regular backups

SECURITY AND PRIVACY ALIGNED

The pandemic saw businesses pivot to alternative, digital strategies and supply chain adjustments to keep business continuing to operate without major disruption. Boards began to step up their oversight of cybersecurity and data privacy practices, which put both of these topics into the spotlight. Cybersecurity and data privacy were cited by directors as the most relevant governance issues to their corporate strategy in 2021. Data governance is often noted as overlapping with cybersecurity. However, data governance includes compliance with privacy legislation and regulation and how businesses legally process, store and use personal data. Wider stakeholders are paying greater attention to how their data is used, which can pose a significant reputational risk for an organisation. Hence, cybersecurity and privacy need to be handled carefully and in unison.

Boards should ensure an organisation has a robust data governance framework in place, as well as a cybersecurity framework to improve transparency on what data is being collected, stored and used. Through a board's sub-committee structure, data governance should be appropriately delegated to a committee, usually the Audit committee, to maintain effective oversight and identify critical risks and related controls to an organisation's data privacy, as well as cybersecurity.

Suspected data breach

Under the Notifiable Data Breach Scheme (NDB) any organisation or agency covered by the 1988 Privacy Act must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved.

A data breach occurs when personal information an organisation or agency holds is lost or subjected to unauthorised access or disclosure. For example, when:

- a device with a customer's personal information is lost or stolen
- a database with personal information is hacked
- personal information is mistakenly given to the wrong person

The notification to individuals must include recommendations about the steps and organisation should take in response to the data breach. NDBs and Privacy requirements more broadly are discussed in further detail in [Chapter 22](#).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

CYBERSECURITY AND DATA PRIVACY IN BUSINESS CONTINUITY PLANS

No two organisations are the same, therefore, there is no 'one-size-fits-all' business resiliency plan. Despite cyber incidents being complex and not always having the same attributes, incident management is a critical component of an overall cyber risk program and the effectiveness of an incident response plan. It is important to have a business continuity plan that tests cybersecurity and data privacy responses under different scenarios that are regularly reviewed, at least annually, to reflect changes in the external environment.

In addition, organisations should clarify which business leaders are accountable for business continuity and decision-making if an incident were to occur. This is particularly important if an incident involves third parties who have to be notified promptly.

CRITICAL SUCCESS FACTORS

- The roles of directors and the board in overseeing cybersecurity and cyber incident responses are clearly defined and documented.
- Accountabilities and reporting lines for cybersecurity management are clearly defined and well understood.
- There is regular enterprise-wide cyber risk communication.
- There is a comprehensive awareness framework that focusses on effective communication throughout the organisation.
- The organisation is addressing the key issues and ensuring staff at all levels are receiving clear and relevant messages about cybersecurity and data privacy.
- The key issues and concerns around cybersecurity are clearly communicated in meetings and in communication from management.

- The board (and sub-committees) receive the right reports, such as a cybersecurity scorecard to effectively manage cybersecurity risks.
- An organisation is transparent in informing its stakeholders about cybersecurity risks and privacy concerns, including how data is used and stored.
- Cybersecurity and data privacy are included in business continuity plans and take into consideration security for the Cloud.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- Cybersecurity Planning Guide – Federal Communications Commission (USA), <https://transition.fcc.gov/cyber/cyberplanner.pdf>
- KPMG, Empowering Your business strategy with Cybersecurity: <https://home.kpmg/gr/en/home/services/advisory/risk-consulting/it-advisory-services/cyber/empowering-business-strategy-with-cybersecurity.html>
- KPMG, CISO – From enforcer to influencer <https://thenews.au.kworld.kpmg.com/management-consulting/ciso-from-enforcer-to-influencer/>
- <https://assets.kpmg/content/dam/kpmg/au/pdf/2018/digital-supply-chain-hype-and-risks.pdf>
- KPMG, Critical Infrastructure reforms <https://home.kpmg/au/en/home/topics/critical-infrastructure-reforms.html>
- Cyber and Infrastructure Security Centre, <https://www.cisc.gov.au/resources>
- KPMG, The changing shape of ransomware, <https://assets.kpmg/content/dam/kpmg/au/pdf/2021/the-changing-shape-of-ransomware-au.pdf>
- Australian Cybersecurity Centre, Essential Eight, <https://www.cyber.gov.au/acsc/view-all-content/essential-eight>

For further information please contact:

**Greg Miller**

**Partner, Cyber Security
– Critical Infrastructure
& Government Lead
KPMG Australia
gmliller3@kpmg.com.au**

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

24. Data Privacy and Personal Information

Privacy legislation in Australia and around the world continues to evolve and strengthen, bringing data governance and the management of personal information to the forefront of many board agendas. The Australian privacy legislative environment is expected to further tighten, with the Privacy Act 1988 (Cth) (the 'Privacy Act') currently undergoing significant reform in attempt to bring Australian more in line with overseas jurisdictions. The Privacy and Other Legislation Amendment Act 2024 was passed by the Australian Parliament in November 2024 and received Royal Assent on 29 November 2024. The majority of the Act's provisions came into effect on 10 December 2024, with certain provisions, such as the statutory tort for serious invasions of privacy, commencing on 10 June 2025, and others related to automated decision-making having a two-year grace period, ending 10 December 2026.

In this chapter

- Privacy in Australia
- International privacy regulation and the impact on Australian organisations
- How do organisations manage privacy risks?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should consider asking

1. What privacy regulations are applicable to the organisation (important to check international jurisdictions and local state laws)?
2. What are the data privacy risks faced by the organisation?
3. Do management have a clear understanding of the information lifecycle, from collection, through to use, disclosure, retention and destruction?
4. Does the organisation maintain an accurate and up-to-date data inventory or data map?
5. Is the organisation adequately prepared to deal with a data breach involving personal information? Do we have the ability to quickly identify and manage data breaches?
6. What training and awareness activities are being undertaken to ensure staff throughout the organisation are aware of applicable privacy compliance obligations and risks?
7. Is privacy embedded in the organisation's risk management framework?
8. Does the organisation have appropriate controls in place to help assess and manage privacy risks arising from organisational change or projects (e.g. conducting privacy impact assessments)?
9. Does the organisation understand what third parties are involved in PII processing activities and the controls in place to protect this information (e.g., appropriate contractual agreements, ongoing assurance activities, off-boarding, etc.)?
10. Does the board or relevant committee receive appropriate oversight on privacy/data governance, controls and incident/complaint reporting?
11. How is the organisation preparing for the upcoming Australian privacy regulatory reforms?
12. How organisation is embedding privacy and data protection at the onset i.e. at the stage of conceptualisation of any new digital initiative, transformation, product and services.
13. What safeguards are in place to protect personal data from internal threats (e.g., employee misuse or negligence)?
14. Does the organisation have effective processes in place to handle privacy complaints and respond to individual rights (e.g., access, correction, deletion, objection)?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- Privacy is not on the boardroom agenda.
- Privacy/data risk is not specifically included in assessing business and operational risk.
- Accountability for privacy or data governance is unclear and/or undefined.
- Lack of visibility of data holding within the organisation and with the third parties.
- The organisation does not have a data breach response plan with clear actions and accountabilities.
- Inadequate mechanisms for individuals to exercise their privacy rights (e.g., access, correction, or deletion requests)
- No clear process for managing cross-border data transfers and ensuring compliance with international privacy standards.
- Projects involving the use of customer or other personal information are not considering privacy risks.
- Failure to conduct vendor due diligence or monitor third-party compliance with privacy requirements.
- The organisation does not adopt a 'privacy by design' approach within its operations.
- Personal information is not destroyed or disposed of when it is no longer needed for the purpose it was collected for, or it is not being retained in accordance with applicable retention laws.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

PRIVACY IN AUSTRALIA

Australia's privacy framework is supported by a sophisticated blend of Federal, State, Territory, and sector-specific laws, including those regulating health and telecommunications. Under the Privacy Act 1988 (Cth), the Notifiable Data Breach (NDB) scheme mandates serious data breaches be reported to the OAIC.

Major reforms occurred in:

- 2014: Introduction of the Australian Privacy Principles (APPs)
- 2018: Establishment of the NDB scheme

The Privacy and Other Legislation Amendment Act 2024 marked the first tranche of significant updates, enacting measures like a statutory tort for privacy, tiered penalties, automated decision-making transparency, doxxing offences, enhanced enforcement powers and data security obligations, and a whitelist for international data transfers. Most of these changes came into effect from 10 December 2024, with further provisions phasing in through mid-2025 and 2026.

While these updates represent substantial steps forward, further reform remains in progress. Proposals such as expanding coverage, sharpening processing standards, and extending enforcement tools await legislative action.

Changes to the Privacy Act in 2024 are based on overseas regulations such as the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These changes represent a significant reshaping of privacy laws in Australia.

An overview of the Privacy Act

In Australia, the Privacy Act governs how applicable organisations must handle personal information. The Privacy Act applies to private sector organisations with a turnover of more than \$3 million, as well as most Commonwealth Government agencies.

The Act includes a number of components, including the 13 Australian Privacy Principles (APPs) that are used to govern most organisations, as well as some specific regulations for organisations involved in credit reporting, health and medical research, and the use of tax file numbers.

The Australian Privacy Principles

The APPs are the heart of Australia's privacy regulatory framework and establish the governance standards, rights and obligations for APP entities relating to:

- collection, use and disclosure of personal information
- accountability and governance
- integrity of personal information
- the rights of individuals to access their personal information (which organisations must facilitate).

As principle-based legislation, the APPs incorporate little in the way of proscriptive regulatory requirements. APP entities are, therefore, left with a degree of flexibility in determining the best way to meet and uphold the requirements established by the 13 APPs.

The APPs are also technology neutral, meaning that the principles apply equally to information collected and stored on an organisation's CRM software, as information recorded as handwritten notes and stored in an employee's desk drawer.

Mandatory data breach notification requirements

In addition to the APPs, Australian Privacy legislation also incorporates mandatory data breach notification obligations. This legislation is known as the NDB scheme and applies to all APP entities. The NDB scheme requires regulated entities to notify particular individuals and the OAIC of all eligible data breaches.

An eligible data breach is a breach that is likely to result in serious harm to any of the individuals to which the information in the data breach relates. This requires three criteria to be met:

1. There is unauthorised access, disclosure or loss of personal information.
2. The breach is likely to result in serious harm to one or more individuals.
3. Remedial action has not been able to prevent the likely risk of serious harm.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Accordingly, not all data breaches are notifiable. This highlights the importance for organisations to have clearly established mechanisms in place to quickly identify potentially notifiable data breaches. If organisations can quickly identify, assess and remediate data breaches, serious harm to individuals may be avoided, thereby removing the requirement to notify and be subject to the negative publicity and regulatory scrutiny that may follow.

Insights from NDB reporting

The OAIC releases regular statistics on the leading causes of notifiable data breaches. This information is a valuable resource for organisations as it highlights common issues or mistakes made by organisations, thereby providing insight into where organisations may require strengthening.

From July to December 2024, the OAIC received 595 data breach notifications, bringing the total for the year to 1,113 breaches—the highest annual total since the NDB scheme began in 2018, a 25% increase compared to 2023. Malicious or criminal attacks accounted for the largest share, comprising 69% of breaches, with cybersecurity incidents, such as phishing and ransomware being particularly prevalent. Human error remained a significant contributor, commonly involving scenarios like emailing personal information to the wrong recipient. The health sector was the most frequently notifying sector (accounting for ~20% of total breaches), followed by Australian Government agencies (~17%).

This highlights the fact that good privacy management necessarily involves more than just cyber security, and the importance of preventative controls like the provision of training and awareness for all staff, particularly those in high-risk roles.

Consumer Data Right

The Australian Consumer Data Right (CDR) regime commenced in July 2020, with the aim of providing consumers with greater access to and control over their data, along with improving consumers' ability to compare and switch between products and services. The CDR enables more competition between service providers, leading not only to better prices for customers but also more innovative products and services.

The CDR endeavours to provide greater choice and control for Australians over how their data is used and disclosed. It allows consumers to access particular data in a usable form and to direct a business to securely transfer that data to an accredited data recipient.

Under the regime, 'CDR consumers' (both individuals and businesses) are given a right to access, and direct accredited third parties (ADRs) to access and use, information held about that consumer by a data holder.

The security and integrity of the CDR regime is maintained by 13 privacy safeguards, contained in the *Competition and Consumer Act 2010* (Cth) and supplemented by the Consumer Data Rules. These privacy safeguards set out the privacy rights and obligations for users of the scheme, including the requirement for informed consent to collect, disclose, hold or use CDR data.

The Consumer Data Right is designed to be an economy-wide right, with rollouts proceeding sector by sector. It was first implemented in the banking sector, followed by energy. The non-bank lending sector has now also been designated, with the updated CDR Rules effective from March 2025. Product data sharing obligations for non-bank lenders begin on 13 July 2026, followed by consumer data sharing rolling out in phases between 9 November 2026 and 13 September 2027.

Digital ID powering the future of Australia's digital economy

Australia is indeed progressing toward an economy-wide Digital ID system designed to help protect individuals' identity information and enable secure online identity verification with both government services and businesses.

- The Digital ID Bill 2024 together with the Digital ID (Transitional and Consequential Provisions) Bill 2024 have passed both houses of Parliament, the Senate in March and the House of Representatives shortly thereafter marking a major legislative milestone.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

- These Bills establish a legislative framework for a federated Digital ID ecosystem, including an accreditation scheme for providers, expanded scope for the Australian Government Digital ID System (AGDIS), and strong privacy and security safeguards.
- The legislation is expected to receive Royal Assent and for the Digital ID Act 2024 (including supporting rules and standards) to commence on 1 December 2024. From 1 December 2024, government and state/territory services can apply to join the system as relying parties; from December 2026, private sector entities will also be able to apply for accreditation.

INTERNATIONAL PRIVACY REGULATION AND THE IMPACT ON AUSTRALIAN ORGANISATIONS

Privacy regulation in jurisdictions outside of Australia are constantly changing and evolving. Most notably, the arrival of the GDPR in early 2018 represents the most significant and far-reaching privacy legislation to date.

The European General Data Protection Regulation

The GDPR was introduced within the European Union to create a standard approach to data privacy across all member states and is widely regarded as the most stringent and comprehensive privacy legislative regime. While some elements of the GDPR overlap with the Privacy Act, there are several key differences, including:

- the right for data subjects to revoke their consent to use their personal information at any time
- more stringent requirements relating to the provision of consent
- notification of eligible data breaches within 72 hours (instead of the 30 days allowed under the Australian NDB Scheme)
- limitations on transferring personal information to locations outside of the EU
- much higher fines and regulatory enforcement powers, including up to EUR20 million or up to 4 percent of global turnover (whichever is higher) in certain scenarios
- application to organisations that operate in international jurisdictions.

Applicability of the GDPR to Australian organisations

The GDPR is notable for its extraterritorial applicability. The GDPR can have applicability to organisations that operate outside of the EU in two situations:

1. Where data processors or controllers have an establishment within the EU.¹ In this scenario the GDPR will apply regardless of whether personal data is actually processed in the EU or elsewhere.
2. Where data controllers or processors are located outside of the EU, but their processing activities relate to goods or services offered to individuals within the EU or monitor the behaviour of individuals within the EU.

Other international privacy legislation

While the GDPR is often referred to as the most significant piece of international privacy legislation for Australian organisations, other jurisdictions are quickly reviewing and updating their regulatory schemes.

United States: the California Consumer Privacy Act (CCPA), effective since January 2020, was one of the first comprehensive state-level privacy laws in the U.S. with an extraterritorial application. The CCPA applies to businesses that collect personal information relating to residents of California (regardless of where the business is located). The CCPA grants residents rights similar to those in the GDPR, such as the right to access and delete personal information, and imposes obligations on businesses around transparency and data handling.

The California Privacy Rights Act (CPRA), which came into effect in January 2023, builds on the CCPA by enhancing consumer rights and establishing a dedicated California Privacy Protection Agency for enforcement. Other U.S. states, such as Virginia, Colorado, and Utah, have also enacted their own privacy laws, each with unique provisions.

¹ Data controllers are parties that say how and why personal data is processed. Data processors are parties that act on behalf of a data controller.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

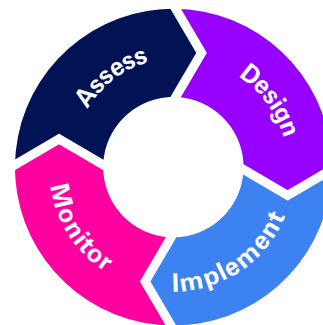
CONTACT US

New Zealand: The Privacy Act 2020 came into force on December 1, 2020, representing a significant update to New Zealand's privacy framework. Key reforms included:

- mandatory reporting of data breaches
- providing the Privacy Commissioner with the power to issue compliance notices to require or prevent organisations from doing something
- introduction of new offences and increasing fines.

*KPMG assists clients in complying with these complex privacy regulations through the four phases of the privacy management lifecycle: **Assess, Design, Implement, Monitor***

- Privacy maturity assessment
- Privacy audits
- Third party privacy assessments
- GDPR programme readiness
- CDR programme readiness
- Privacy management framework
- Privacy policies
- Data segregation
- Records management framework
- Privacy impact assessments



- Ongoing operations
- Privacy office support
- Incident management
- Data breach response and investigation
- Regulatory management
- Risk and obligations registers
- Data inventory
- Sensitive data finder
- Training and cultural change
- Data strategy, governance and technology innovation

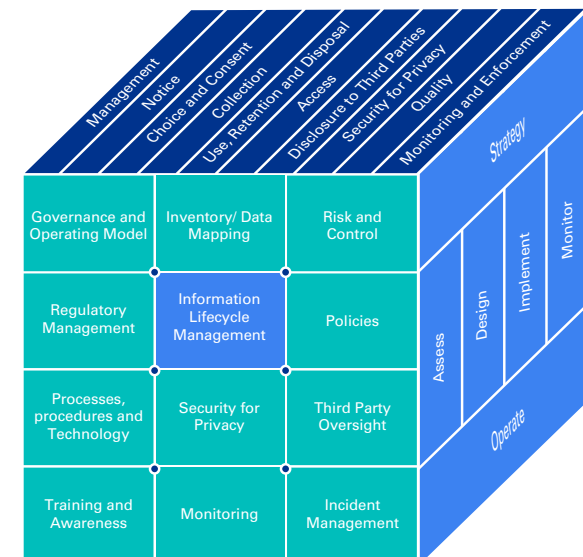
HOW DO ORGANISATIONS MANAGE PRIVACY RISKS?

Privacy risks are quickly becoming one of the most monitored risks for an organisation. Properly managing privacy risks requires a commitment and focus from staff throughout the organisation. This is due to the fact that privacy risks can surface not only from IT system failures or cyber security vulnerabilities, but also from a simple email being sent to an incorrect recipient.

KPMG Privacy Management Framework

The KPMG Privacy Management Framework is made up of 12 elements that align to the Generally Accepted Privacy Principles (GAPP) framework, which underpins most privacy legislation and regulation around the world. It offers a logical framework from which to identify, assess and manage privacy risks, and from which a range of privacy controls can be established to help manage privacy risks.

The KPMG Privacy Management Framework



FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- KPMG Australia Privacy & Data Protection Services, <https://home.kpmg/au/en/home/services/advisory/risk-consulting/privacy.html>
- KPMG Data Protection Navigator, <https://home.kpmg/au/en/home/services/advisory/risk-consulting/privacy/data-protection-navigator.html>
- Global Privacy Law and DPA Directory, <https://iapp.org/resources/global-privacy-directory/>
- OAIC Notifiable Data Breaches Report: July-December 2024: <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2024>
- OAIC guidance for Australian Organisations on the GDPR, <https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation/>
- OAIC guidance on how to respond to a data breach, <https://www.oaic.gov.au/privacy/data-breaches/respond-to-a-data-breach-notification/>
- The Digital ID (Transitional and Consequential Provisions) Bill 2024, Digital ID Bill 2024 – Parliament of Australia (aph.gov.au)

For further information please contact:

**Kelly Henney**

**Partner, Privacy & Data Protection,
Trusted AI Lead
KPMG Australia
khenney@kpmg.com.au**

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

25. Human Rights and Modern Slavery

Human rights reporting and due diligence requirements are growing around the world, and the global community of investors, governments, employees, and consumers increasingly expects enhanced human rights performance.

All organisations are exposed to human rights risks in their operations and supply chain. These are risks where people may experience or have experienced harm as a result of an organisation's decisions or practices.

Directors have regulatory responsibilities for transparent mandatory reporting on modern slavery risks in Australia, and there is international acceptance that businesses take a human rights due diligence approach to identifying, managing and reporting on these risks. A key difference between human rights due diligence and traditional business due diligence and risk management is that human rights due diligence focuses on risks to people rather than risks to the entity. Human rights issues and modern slavery can occur in every industry and sector and has severe consequences for victims. Mismanagement of human rights and modern slavery risks also decreases investor confidence, undercuts responsible business, and poses significant legal, commercial and reputational risks to entities.

In this chapter

- The emergence of human rights as a business risk
- Legislation
- Challenges of managing modern slavery risks
- The role of the board
- Governance reporting and KPIs

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. Is the company able to report at a group level on behalf of all subsidiaries and across all geographies?
2. Does the board receive regular updates on changes to the structure, operations and supply chain of the company?
3. Has the board determined if its approach to publicly releasing detailed information about its operations and supply chain is aligned with good practice?
4. Do board members understand what behaviours and practices constitute modern slavery and likely risk factors for the business and sector in this regard?
5. Has the board included modern slavery risks on its risk register?
6. Has the board established accountabilities for the identification and management of modern slavery risk through its committees or executive reports?
7. Has the board established KPIs for managing modern slavery risk?
8. Does the company express its commitment to respecting human rights, including modern slavery, through a board approved public statement of policy?
9. Has the board introduced assurance measures for modern slavery due diligence activities?
10. Does the board monitor and review its human rights and modern slavery programs and their implementation?
11. Has the company benchmarked itself against good practice to determine its current maturity and guide its future ambition?
12. Have the company's management systems and controls uncovered any instances of modern slavery and, if not, are they robust enough to do so?
13. Does the company have grievance mechanisms and formalised remediation processes in place that allow internal and external stakeholders to raise complaints in respect of modern slavery and human rights concerns in its value chain?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- The company has no public commitment to respect modern slavery or human rights.
- There is no evidence of risk assessment to identify and prioritise modern slavery or human rights risks or impacts.
- There is no reporting to the board on the company's approach to responsible business practices.
- There are no accountabilities assigned for human rights or modern slavery within the company.
- The company's risk management does not include human rights or modern slavery risk related considerations or screening criteria.
- The company has exposure to high-risk geographies, high-risk categories, risky business models or vulnerable populations.
- The company has been associated with human rights related abuses.
- The company does not have grievance mechanisms, or does not make its grievance mechanisms accessible to external stakeholders.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

THE EMERGENCE OF HUMAN RIGHTS AS A BUSINESS RISK

In 2011, the global community came together to develop the United Nations Guiding Principles on Business and Human Rights,¹ which explicitly recognise the responsibility of businesses to address and manage their human rights risks and impacts. Since the unanimous adoption of the Principles by the Human Rights Council, numerous countries around the world have enacted modern slavery reporting legislation requiring businesses to report publicly on their human rights due diligence in relation to modern slavery risk. In addition to modern slavery reporting requirements, a growing number of jurisdictions have enacted mandatory human rights due diligence laws.

The global regulatory landscape now requires business to shift thinking from a traditional risk-to-business approach to an approach that puts risk-to-people at the centre of risk management efforts.

Most of the world's major businesses now have formal commitments and management approaches to respecting human rights. Stakeholder expectations are elevated, with investors, shareholders, unions, regulators, and civil society increasingly requiring visibility over corporate social performance and how they are addressing the 'S' in ESG, which is seen as the pillar that is about impacts on people and communities.

For example, the Corporate Human Rights Benchmark, which counts investors among its founders, rates 100 of some of the world's largest listed companies according to their publicly reported approach to human rights.

The retail and resources sectors led the corporate world's response to social risk, having been forced to respond by retail's reliance on base-skill labour and the significant impacts on communities from resource development and extraction. Now, human rights reporting and due diligence requirements along with significantly increased expectations that boards will understand and manage non-financial risks, is challenging all sectors to put respect for human rights on the agenda.

¹ https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

AUSTRALIAN LEGISLATION

In 2018, Australia introduced the *Modern Slavery Act 2018* (Cth), which requires reporting entities to publish an annual statement about what they are doing to manage the risk of modern slavery in their operations and supply chains. The Act follows the introduction of similar legislation in the UK and reflects Australia's commitment to develop regulatory frameworks to prevent the exploitation of workers globally. The Act requires entities with over \$100 million in consolidated revenue to publish an annual modern slavery statement. The board must approve the annual modern slavery statement, which is published on a central government register.

On 25 May 2023, the government tabled a report on the statutory review of Australia's Modern Slavery Act, which reviewed the first three years of the Act's operation. The review was conducted in accordance with s 24 of the Act and was led by Professor John McMillan, AO. The review made 30 recommendations for government consideration to strengthen the Act. Key recommendations made in the review included reducing the reporting threshold to \$50 million, introducing penalties for non-compliance with the reporting requirements, introducing due diligence requirements and the establishment of a federal Anti-Slavery Commissioner. On 28 May 2024, Parliament passed the Modern Slavery Amendment (Australian Anti-Slavery Commissioner) Bill 2023, establishing an independent Commissioner at the federal level.

New South Wales also introduced modern slavery legislation, which took effect on 1 January 2022. The NSW legislation was passed after two years of review and amendment to ensure it could effectively operate alongside the Commonwealth law. It requires public entities in NSW (including more than 400 agencies and local councils) to take reasonable steps to address modern slavery risks in their operations and supply chains. The legislation also established an Anti-slavery Commissioner for New South Wales. Dr James Cockayne commenced in this role 1 August 2022. The Commissioner's functions include:

- promoting anti-slavery actions
- identifying and supporting survivors
- monitoring the effectiveness of anti-slavery laws and policies

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

- supporting public entities to tackle modern slavery risks in operations and supply chains
- providing advice and training
- raising community awareness about modern slavery.

A short history on business and human rights risks in supply chains

Business impacts on human rights has been a subject of societal expectations as early as the 19th century when the British public experienced an anti-slavery movement protesting the use of slaves in the Caribbean producing sugar for British consumption. The more recent focus on corporate accountability in this regard began in the mid-1990s, in response to significant human rights violations in the retail sector, including the use of 'sweatshop' labour and the 2013 Rana Plaza disaster in Bangladesh, which led to the death of over 1,000 people. In response, companies like Levi's, Nike, The Body Shop International and Ben & Jerry's established supplier codes of conduct and controls for testing conformance with those codes to mitigate labour-related risks. These global brands also started to commission supplier audits that looked at areas such as labour practices, environmental performance, and animal welfare. As a result, there is today a body of over 30 years of work to address human rights risks and impacts in the supply chain. Despite this, and the growing responsible business expertise and services, many businesses are still immature in their management of these types of risk. However, both expectations and regulations continue to require enhanced human rights reporting and performance. For businesses more advanced in their journey, there is an increasing recognition of the need to go 'beyond compliance' and 'beyond audit' to manage risks in a meaningful way that is focused on preventing harm to people. This includes adopting a collaborative approach to supplier engagement; developing whole of business human rights strategy and risk appetite based on 'risk to people' to guide a human rights due diligence for salient issues (such as modern slavery); engaging with external stakeholders including affected rightsholders; and innovative use of technology to secure and maintain trust across the value chain.

CHALLENGES OF MANAGING MODERN SLAVERY RISKS

In addition to driving improved business practice through transparent reporting, there is growing recognition that industry-wide and multi-stakeholder approaches are an important part of addressing the root causes of modern slavery. This is why there are a growing number of collaborative responses. Some sectors such as retail, property and mining have come together with shared responses to managing supplier platforms, and specific issues are targeted through multi-stakeholder initiatives.

Challenges that collaborative approaches seek to target:

- The complexity of global supply chains and the heavy reliance on agents makes it difficult for organisations to have clear oversight and influence over key areas of exposure.
- Traceability is challenging in the supply chain which diminishes accountability. There are more and more technology-enabled traceability products and services being offered in the market to meet this challenge.
- Geopolitical issues, such as mass migration, result in an increase in the supply of vulnerable low-skill labour.
- Historically there is weak understanding or engagement at senior executive and board level, due to labour practices and supply chain issues having a greater role in operational, rather than strategic, functions.
- The board has limited visibility over the entire supply chain. Additional resources and hence expenditure may be required to monitor this risk.
- Ability and time to respond to new legislation.
- Capacity and ability of staff to address impacts.
- Aligning human rights with values and culture.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Limitations of supply chain auditing

One control in managing supply chain risk is supply chain auditing. This involves setting company-specific standards or subscribing to industry or other multi-stakeholder established standards and auditing supplier performance against those standards. Suppliers and their workplaces are then subjected to a range of audits that can be conducted by the customer or by a third party. These audits typically look at the management approach to labour practices and should always involve worker interviews.

Audits can only ever be a diagnostic tool at a point in time. Successful risk management within the supply chain is not solely a point in time assessment, but rather, it ties together an organisation's human rights and supply chain touchpoints and, in the process, establishes an overall understanding of the nature of the supplier and the relationship with it. Achieving this can be a challenge when there are many tiers in the supply chain and the tendency has been to outsource supply chain risk.

Whilst the auditing of human rights practices is possible, there are high levels of audit fraud. For example, the stakes for failing an audit of human rights practices can be high, perversely creating a compelling reason to conduct audit fraud and facilitate auditor corruption. As a result, auditing should only be regarded as one potential component in a full program of human rights risk management.

A meaningful, ongoing response to human rights risk includes a collaborative approach to supplier engagement and capability building and is targeted to the areas of highest risk of harm to people.

THE ROLE OF THE BOARD

The board has oversight of risk. A critical function of the board is to understand risk to people as part of non-financial risk management. Increasing stakeholder and shareholder activism and scrutiny of the board's view of environmental, social and governance issues will continue to drive the need for directors to understand and take an active role in overseeing human rights risk management. Organisations are increasingly judged on their performance in non-financial risk management, and it is up to directors to ensure they are proactively overseeing risk management and developing strategic responses in this context.

Specifically, with respect to modern slavery risk, the board should ensure that:

- There is a board-approved human rights or modern slavery policy commitment.
- Behaviours and practices that constitute and facilitate modern slavery are understood across the business.
- Modern slavery risk is identified, assessed and mitigated.
- Modern slavery risk is included on the business risk register.
- Accountabilities for the identification and management of modern slavery risk through its committees or executive reports are established.
- The business is demonstrating progress in its reporting against the Australian mandatory reporting criteria and preparing for mandatory due diligence.
- A risk management program is embedded within the company that:
 - addresses the areas of highest risk to people in the supply chain and operations of the business
 - details the expected values and behaviours of business personnel with respect to human rights issues
 - develops objectives and targets for improvements in risk management and its effectiveness, including relevant KPIs and metrics for reporting performance

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

- creates clear standards that the company expects suppliers and business partners to meet and provides support for them to do so
- is regularly reviewed and tracked against good practice.
- Regular reports are provided to the board that monitor performance and highlight any emerging issues.
- Regular consultation with external stakeholders, including affected rightsholders, informs continuous improvement of risk management activity and business understanding of the experience and root cause of modern slavery.
- Human rights risk considerations are built into investment decision-making processes. The effectiveness of the company's approach to managing modern slavery risk is measured over time.

The global evolution of human rights regulation

From reporting to mandatory human rights due diligence

Since the introduction of the seminal UN Guiding Principles on Business and Human Rights (UNGPs) in 2011, multiple jurisdictions across the world have regulated to make business more accountable for human rights impacts, including modern slavery. Initial legislation tended to focus on the imposition of reporting requirements.

With increasing recognition that reporting alone is not producing the changes intended by lawmakers, and increasing stakeholder expectations, a growing number of jurisdictions are now strengthening regulation through the enactment of mandatory modern slavery and/or human rights due diligence laws, as well as import bans.

In Europe, multiple jurisdictions including Germany, France, Sweden and Switzerland have imposed due diligence requirements. Most significantly, in May 2024, the EU Corporate Sustainability Due Diligence Directive was passed, requiring EU companies (or those operating in the EU) with more than EUR450 million turnover, to undertake mandatory human rights (and environmental) due diligence in respect of their operations and supply chains.

The CSDDD provides for penalties for non-compliance and also contemplates civil liability for damage caused to a person, where the company has failed to comply with its due diligence obligations. EU countries are required to transpose the CSDDD into local laws in stages, with very large companies (more than EUR1.5 billion turnover) to be in scope from 2027. While most companies outside the EU are not directly subject to the CSDDD, the laws will have global impact, as EU companies subject to CSDDD requirements will require their suppliers and business partners to demonstrate that they also have systems of due diligence in place, effectively cascading down requirements.

Other relevant laws include importation bans, such as the US *Uyghur Forced Labor Prevention Act* (UFLPA) which prohibits the importation of goods mined, produced, or manufactured wholly or in part in Xinjiang, applying a rebuttable presumption that such goods are manufactured with forced labour. Similarly, in November 2024, the EU Parliament approved the Forced Labour Regulation (FLR) enabling the EU to prohibit the sale, import, and export of goods made using forced labour.

The human rights implications of artificial intelligence (AI) is another area of increased regulatory focus. Recognising the potential human rights risks, the recently enacted EU AI Act requires entities to conduct fundamental rights impact assessments in respect of specified high-risk AI systems.

Together, these developments reflect a growing regulatory and commercial expectation that human rights due diligence is integrated into a company's systems of governance and control.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

GOVERNANCE REPORTING AND KPIS

As the Australian and global regulatory environment evolves, reporting to the board on human rights and modern slavery risk in operations and the supply chain will become increasingly significant.

Meaningful reporting will offer directors the necessary data to show that their business is appropriately identifying and managing modern slavery risks. Directors should proactively seek this information if they are not already receiving it. If they are provided with this information regularly, they should ensure that they understand the issues well enough to ask strategic questions that contribute to a cycle of continuous improvement and alignment with good practice in human rights due diligence.

Meaningful board-level reporting on human rights, including modern slavery, includes:

- **A clear objective.** Focus on keeping the board informed on risk and performance issues, and on building board capability to support strategic conversations. Regular reports should include performance measures, whilst capability-building reports or sessions should be built into the board's agenda as part of broader risk and strategy considerations.
- **Qualitative and quantitative metrics.** These include lead and lag metrics, as quantitative lag metrics alone limit the board to addressing minimum expectations only. Conversely, lead metrics can shift the board's focus to the development of broader, preventative measures. Data should measure performance, including effectiveness over time, and support strategic conversations towards continuous improvement.

Elements of good-practice board reporting include:

- a dashboard with key lead and lag indicators and exception reporting (e.g. number of critical non-conformances that are overdue for close-out)
- results of up-to-date salient issues processes to focus on those areas that strategically matter and where the risk to people is greatest

- key focus areas for improvement in the coming 12 months
- emerging human rights trends and developments relevant to the business.

For supply chain concerns, dashboard indicators could include:

- the number of new suppliers onboarded into the risk management program (this could be expressed as a percentage of the total number of new suppliers)
- the percentage of suppliers in the risk management program that have completed a self-assessment questionnaire
- the percentage of suppliers in the risk management program that have gone through a risk assessment to determine the level of human rights risk
- the percentage of suppliers in the risk management program that have a current, valid third-party ethical sourcing audit report
- the percentage of suppliers within the program that have open non-compliances waiting to be closed
- the percentage of those with open issues that are past their due date for closing non-compliances
- the number and type of supplier employee complaints or enquiries received via factory level helplines and grievance mechanisms, remembering that receiving no complaints is not usually an indicator of success
- the number, and brief description, of ethical sourcing related initiatives (involvement in industry working groups, developing tools to help suppliers deal with second tier suppliers, any country or product category with specific initiatives/partnerships).

In addition to the above quantitative indicators the report could also include:

- **Key focus areas for the next period** – a qualitative description of management responses to potential weaknesses (suggested by the dashboard report) or strategic responses to emerging trends.
- **Emerging trends** – a description of emerging areas of relevance and challenge to business operations or supply chains.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Useful resources

- Australian Council of Superannuation Investors, 2019, *Modern Slavery: Risks, Rights and Responsibilities – A Guide for Companies and Investors*, <https://assets.kpmg/content/dam/kpmg/au/pdf/2019/modern-slavery-guide-for-companies-investors-feb-2019.pdf>
- Australian Institute of Company Directors, 2019, *Modern Slavery Risk Oversight*, <https://aicd.companydirectors.com.au/-/media/cd2/resources/director-resources/director-tools/2019/pdf/modern-slavery/07236-5-modern-slavery-oct-19-a4-web.ashx>
- KPMG and the Australian Human Rights Commission, 2021, *Financial Services and Modern Slavery*, <https://assets.kpmg.com/content/dam/kpmg/au/pdf/2021/financial-services-modern-slavery-practical-guide.pdf>
- KPMG and Australian Human Rights Commission, 2020, *Property, Construction and Modern Slavery*, <https://home.kpmg/au/en/home/insights/2020/08/property-construction-modern-slavery-practical-guide.html>
- KPMG and Australian Human Rights Commission, 2021, *Health services sector modern slavery guide*, <https://home.kpmg/au/en/home/insights/2021/11/health-services-modern-slavery-practical-guide.html>
- KPMG and Australian Human Rights Commission, 2021, *Resources, energy and modern slavery*, <https://kpmg.com/au/en/home/insights/2021/12/modern-slavery-risks-practical-guide-resources-energy-sector.html>
- Office of the Anti-slavery Commissioner (NSW), December 2023, *Guidance on Reasonable Steps: NSW Anti-slavery Commissioner's Guidance on Reasonable Steps to Manage Modern Slavery Risks in Operations and Supply-Chains*, <https://dcj.nsw.gov.au/documents/legal-and-justice/anti-slavery-commissioner/due-diligence-and-reporting/guidance-on-reasonable-steps.pdf>
- KPMG, 2024, *Modern slavery: Are you ready for mandatory due diligence? A practical guide to prepare and respond to evolving modern slavery requirements*, <https://kpmg.com/au/en/home/insights/2024/02/modern-slavery-act-prepare-for-due-diligence.html>
- Supplier Ethical Data Exchange (SEDEX), <https://www.sedex.com/>
- amfori BSCI, <https://www.amfori.org/en/solutions/social/about-bsci>

For further information please contact:



Dr Meg Brodie

Partner in Charge, ESG Social
KPMG Australia
megbrodie@kpmg.com.au



Tina Jelenic

Director, ESG Social
KPMG Australia
tjelenic@kpmg.com.au

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

26. Automation and AI

Automation and AI will have a lasting impact on the future of organisations; the result will be far larger and will be deployed much faster than everyone anticipates. With digital business strategy moving to the heart of every business, organisations – public, private, government-owned or not-for-profit – need to consider how they will engage with and incorporate automation and machine learning, or artificial intelligence (AI), into their thinking.

The pace of change, the change in the way in which customers behave and the ethical considerations for automation and AI all require directors to have a strong understanding of this new risk profile, its impact on risk appetite and how these emerging technologies impact their organisation's business model, culture and risk framework.

In this chapter

- Evolution of the revolution
- Artificial intelligence vs machine learning
- Convergence of automation and AI
- Ethical considerations
- Algorithms
- Governance issues associated with automation, AI and machine learning
- Governance in regulatory uncertainty
- The role of the board

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Questions that company directors should ask

1. How can the organisation ensure that the use of AI is aligned with their business goals and ethical principles?
2. How can the organisation ensure that the AI systems are transparent and their decision-making processes are explainable?
3. What is the organisation's policy on employee use of generative AI?
4. Does the organisation have a governance structure for a board and committee to oversee generative AI?
5. Should certain committees have specific oversight responsibilities, including perhaps taking deeper dives into certain aspects of generative AI?
6. What processes are in place to ensure the governance framework is regularly reviewed and updated?
7. Does the organisation have the necessary generative AI-related talent and resources, including in finance and internal audit?
8. Is training of AI going to be implemented for all staff, and is it mandatory?
9. How can the organisation proactively monitor the regulatory environment for AI and ensure compliance with relevant laws and standards?
10. How and when is a generative AI system or model (including a third-party model) to be developed and deployed, and who makes that decision?
11. How does an organisation ensure that AI models are continuously improved and updated throughout their lifecycle to adapt to new data, changing conditions, and emerging best practices?
12. What comprehensive risk management framework is in place to address the potential risks associated with AI, particularly around data privacy, cybersecurity, and compliance?
13. What contingency plans are in place to address potential failures or malfunctions of AI systems?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Red flags

- Thinking data and AI is only a technology capability's problem.
- No KPIs for successful design, implementation and sustainment.
- The project is talked extensively, but the plan to sustain AI driven technologies are not considered.
- There is no consideration of how the board will evaluate, manage and monitor acceptable use.
- There is no consideration for monitoring algorithm patterns, integration and best practices.
- There is no plan to consider risk of using/not using AI.
- Thinking an AI framework is independent of existing data, risk, compliance, cyber and technology frameworks.
- Ethical use of data and AI is not part of data and AI strategy, but an afterthought in risk mitigation.
- Automation and AI have not been discussed as part of risk and strategy discussions or not addressed in a joint context of business and IT strategies.
- Automation and AI are deployed outside a structured automation strategy and operating model.
- No governance frameworks have been developed to monitor or provide assurance about the quality, accuracy or rigour of the outcomes produced by automation and AI.
- Directors are reluctant to consider emerging technologies because they fail to see the relevance to the business.
- The workforce implications of automation and AI innovations across the business are not understood.
- Executives cannot explain the potential or actual impact of automation and AI on the business – and which competitors are leading the space.
- Executives cannot explain their position on transparency versus explainability.
- Innovation is touted as essential but is not supported or invested in by the business.
- Disruption is not on the strategic risk register.
- The appointment of a Chief Digital Officer/Chief Data Officer/Chief Analytics Officer to the executive team has not been considered. The differences in these roles are not understood or discussed.
- Accountability and responsibility are limited to only technology capability.
- There is no budget for innovation and investment in emerging technologies, such as AI, or that budget is not expressly linked to benefits realisations.
- The enterprise has struggled to get the basics right (e.g. poor data quality, very limited or poor quality descriptive and diagnostic BI) or has a history of issues with poor automation or AI outcomes.
- Automation and AI are proposed for operations in high risk, highly regulated, highly visible areas of the organisation or operations in areas with a direct impact on human safety.
- There is a high turnover of technology staff or strategic consultants.
- Customer complaints/returns/credits are rising shortly after implementation.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

EVOLUTION OF THE REVOLUTION

We have entered the fourth industrial revolution. In an age of automation, machine learning, AI, Internet of Things (IoT) connectivity, augmented and virtual reality and robotics. Industries, operating practices and careers will be replaced, recreated or made redundant. New careers and roles will be created that have never before been imagined. This revolution leads many organisations to question what they stand for in the market, how their organisation operates and what this means for their traditional workforce model.

Technology

Even though technology (in the context of mechanising human activity) has been around for centuries, the technological age that we find ourselves in today has seen an unprecedented pace of change in the development and take-up of digital devices designed to make our lives easier. Whether through automated manufacturing processes, bots that write news articles based on streams of internet information, or complex algorithms designed to predict our spending patterns – the opportunities, threats, and the governance required to meet stakeholder expectations are changing.

Technology impacts business models in ways that would have been hard to predict a few years ago. Business models that have grown from 'garages' and own very few 'physical' assets – such as Uber, Airbnb and Facebook – have become the most valuable companies in the world. Things that may not have seemed possible a decade ago are quickly evolving into reality. For example, who would have predicted wearable tech that captures biological statistics that can be downloaded into your (or an organisation's) cloud of data? Who expected Elon Musk to 'solve' South Australia's energy crisis or Twitter bots to influence an election campaign?

Customer experience

This digital revolution is driving change in the way customers interact with an organisation. It creates different expectations of service standards and delivery beyond traditional definitions and measures of success. Machines are also heavily involved in sales maximisation and demand creation, whether through clickbait or complex algorithms that monitor, track, and pre-empt purchasing patterns of consumers (also known as personalised one-on-one marketing).¹

In 2014, global researcher Gartner forecasted that by 2016, 89 percent of businesses would soon be competing primarily on customer experience. By 2020, the customer will manage 85 percent of its relationships with enterprises without interacting with a human.² Most would agree that this prediction has become a reality, and the Covid pandemic has increased the focus on virtual interactions in customer experiences.

Consumer behaviours are expected to change; KPMG's Innovation team also predicts that technology faces the Trust Paradox as we proceed through the 2020s. Around the world, people are both increasingly dependent on but distrustful of how enterprises use digital technology. This distrust will no doubt lead to greater regulatory scrutiny.

Consumer Data Rights (which started in the banking industry and are now moving to the energy sector and beyond) are transferring more power and ownership over personal data from the company to the consumer by enabling customers to freely exchange their data from one provider to another.

¹ Facebook is one of the largest users of these algorithms – see ABC's Four Corners episode, 'Cracking the Code – What Facebook really knows about you', 10 April 2017 (Available on <https://www.abc.net.au/news/programs/4corners>).

² <https://www.gartner.com/imagesrv/digital-marketing/pdfs/agenda-overview-for-customer.pdf>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

The broader role of public trust is also higher on the agenda for many organisations – whose 'bot' or algorithm do you trust? Who do you trust with your data? These are not subtle shifts. These are issues that will generate significant risks and opportunities for all businesses. Boards and directors must understand what it means for their business – strategically and operationally. Every business must consider the impact of platforms, figure out how to leverage them or copy them.

ARTIFICIAL INTELLIGENCE VS MACHINE LEARNING

We use the term AI as an umbrella term to describe computer systems that are able to perform specific cognitive tasks typically requiring human intelligence. Machine learning is the way for AI to learn, and deep learning is a subset of that, using artificial neural networks to mimic brain activities using mathematical processes enabled by high powered computer processing hardware. The proliferation of AI has generally grown with the use of Big Data, and leaps in computing power enabling increasingly sophisticated analytics, machine learning and deep learning algorithms.

Enterprises must actively seek to gain from advances in computer processing power, access to data and the ease of storage driving the developments in AI. Directors and executives will need to have a clear vision. Organisations must have a solid culture to effectively plan and manage this shift to a machine-driven intelligent enterprise.

CONVERGENCE OF AUTOMATION AND AI

Automation and AI can be considered, and deployed, separately. However, they are increasingly convergent technologies and are often deployed together to streamline and scale decision-making across organisations.

Automation (sometimes known as robotic process automation, or RPA) typically replaces human action on a computer system by:

- following a set of pre-programmed steps (think of an ATM's computer determining whether to dispensing cash or not), and/or
- using a trained AI model to determine the next step (think of a marketing system learning customer preferences and sending tailored offers to them).

The benefit and risk of such a system varies greatly and is generally dependent on the level of autonomy, human programming and the nature of the process or decision being automated.



FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

RELATIVE RISK OF A SYSTEM BASED ON ITS ANALYTICS SOPHISTICATION AND AUTONOMY

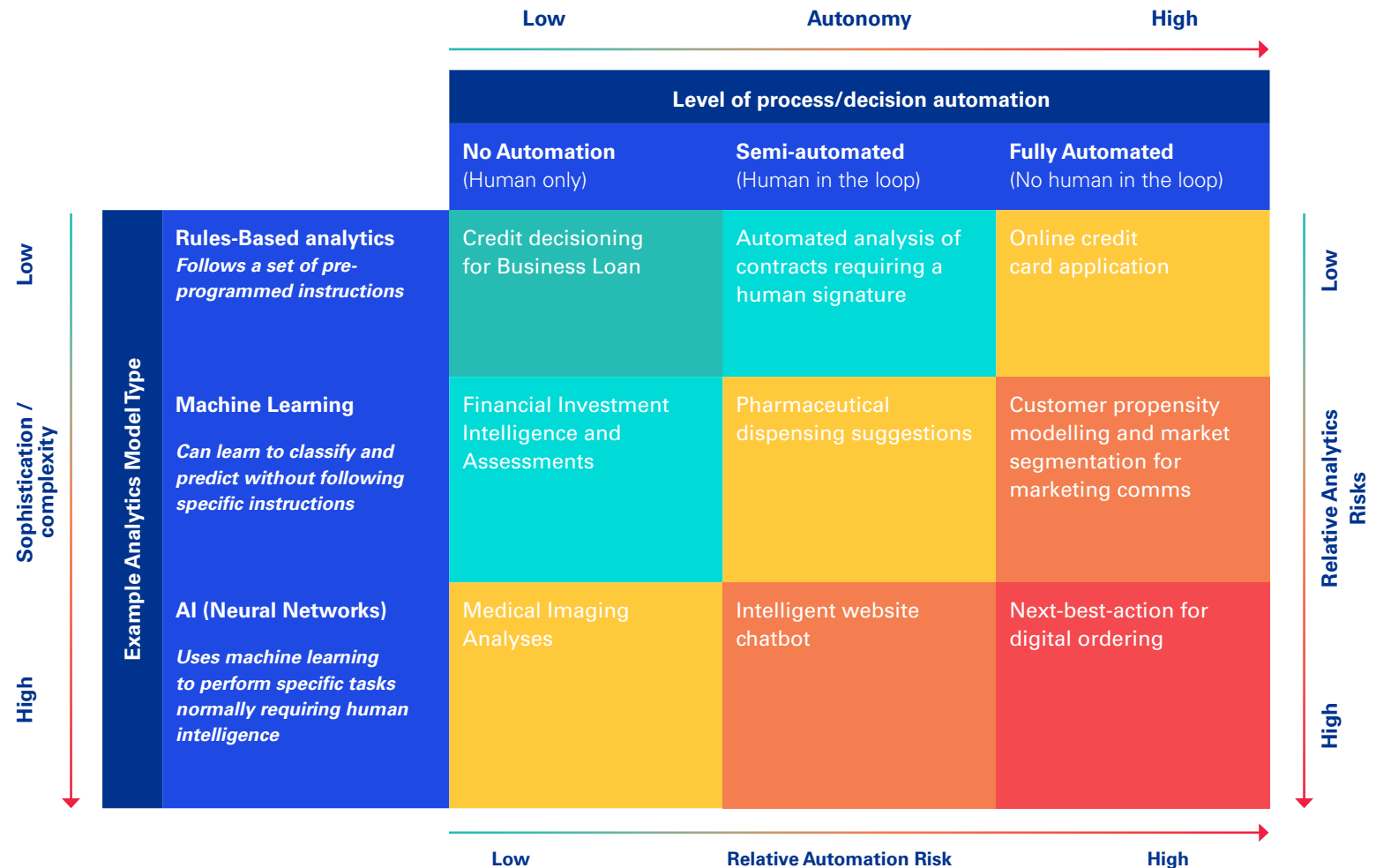


Figure 1: Relative risk of a system based on its analytics sophistication and autonomy. Rules-based analytics are certainly not free of risk as human error in their development and execution can lead to major issues, however, they are generally more transparent and thus easier to audit, control and manage compared to neural networks. The nature of the automation/decision is not depicted here but will also have a significant influence on the overall risk.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ETHICAL CONSIDERATIONS

The rise of automation and AI can raise significant ethical issues for the enterprise and the community, which are being felt in boardrooms across the globe. The World Economic Forum (WEF) has highlighted several ethical considerations associated with the increase in sophistication and adoption levels of AI.³ These are:

- unemployment
- inequality of wealth distribution
- social impacts and lack of human connectedness

- artificial 'stupidity' and poor machine 'learning'
- bias in AI analysis and outcomes
- security against adversaries
- protecting against unintended consequence
- singularity and staying in control of AI
- robot rights – reward and incentives for AI.

From a director's perspective, these issues can raise several governance issues. Most obvious, at present, are those associated with workforce changes, security and social implications.

THE KPMG TRUSTED AI PRINCIPLES



THE KPMG TRUSTED AI PRINCIPLES

What we aim to do

Throughout the KPMG organisation, our approach to trusted AI includes foundational principles that guide our aspirations in this space, demonstrating our commitment to using it responsibly and ethically

Values-Driven	Human-Centric	Trustworthy
We implement AI as guided by our Values. They are our differentiator and shape a culture that is open, inclusive, and operates to the highest ethical standards.	We are embracing AI to empower and augment human capabilities—to unleash creativity and improve productivity.	We strive to ensure our data acquisition, governance, and usage practices uphold ethical standards and comply with applicable privacy and data protection regulations.

³ World Economic Forum, Top 9 ethical issues in artificial intelligence, 21 October 2016, <https://www.weforum.org/stories/2016/10/top-10-ethical-issues-in-artificial-intelligence/>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

THE KPMG TRUSTED AI ETHICAL PILLARS

How we aim to deliver our commitments

At KPMG, our approach to trusted AI rests on ten ethical pillars across the AI lifecycle

	Fairness AI solutions should be designed to reduce or eliminate bias against individuals, communities, and groups.
	Transparency AI solutions should include responsible disclosure to provide stakeholders with a clear understanding of what is happening in each solution across the AI lifecycle.
	Explainability AI solutions should be developed and delivered in a way that answers the questions of how and why a conclusion was drawn from the solution.
	Accountability Human oversight and responsibility should be embedded across the AI lifecycle to manage risk and comply with applicable laws and regulations.
	Data Integrity Data used in AI solutions should be acquired in compliance with applicable laws & regulators & assessed for accuracy, completeness, appropriateness, & quality to drive trusted decisions.
	Reliability AI solutions should consistently operate in accordance with their intended purpose and scope and at the desired level of precision.
	Security Robust and resilient practices should be implemented to safeguard AI solutions against bad actors, misinformation, or adverse events.
	Safety AI solutions should be designed and implemented to safeguard against harm to people, businesses, and property
	Privacy AI solutions should be designed to comply with applicable privacy and data protection laws and regulations.
	Sustainability AI solutions should be designed to be energy efficient, reduce carbon emissions, and support a cleaner environment

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

THE KPMG TRUSTED AI COUNCIL

How we drive principles into practice

KPMG firms are at the cutting edge of AI, playing an active role both in shaping market discussions to help clients and the wider industry to unlock its value and collaborating with stakeholders across the ecosystem to form its governance.

The KPMG Trusted AI Council is a global, cross-functional group that established and will continually review our foundational principles in accordance with evolving regulations and technological advancements. The Council guides how we put our principles into practice, including training KPMG professionals on the ethical and responsible use of AI and addressing emerging matters that may arise.

Workforce changes

As more and more processes and even entire job roles become automated, the current roles that we know today will slowly become increasingly redundant. They will be replaced by new roles and through organic growth. Ethically, this can cause issues for some organisations who have established themselves as employers of choice but are now faced with significant changes in their workforce regarding FTEs, skills, and more 'agile' or flexible work arrangements. But as some roles are disappearing, brand new job roles are already starting to emerge such as Metaverse Engineer and Blockchain Architect.

Directors, as leaders of culture within an organisation, need to be asking management:

- What are the potential impacts of automation and AI on our people?
- How do we balance customer experience, employee experience, profitability and workforce changes in the context of greater automation, cost pressures and social responsibility?
- How do we deal with cultural change and its human impact?
- What do we offer in terms of training and retraining?
- What will our stakeholders think – is cost a bigger driver of consumer spending than organisational behaviour and ethics?

It may come down to how transitions are handled rather than the extent of the transition itself.

Security

Automation and AI can be deployed to enhance security activities. Data security is already a hot topic under the 'cyber risk' banner. Machine-learning algorithms are being used extensively in cyber security to sift through millions of transactions and volumes of network traffic to detect threats. As automation and AI evolve, and we see further advances in what machines are capable of, we must also consider physical security. Drones, for example, are being used for deliveries of goods, driverless cars are being touted as a future delivery service as well – but what does this mean for the physical safety of our customers and citizens – be it from hackers or privacy issues associated with information (text, pictures, personal details, personal preferences, etc.)? Regulatory change is likely to evolve further in these areas, particularly in the context of geopolitics and national security.

Social impact

Despite the increased demand from consumers for greater digital connectivity and 'smart' devices to simplify or streamline our lives, the social impacts of losing human connection are already felt in many parts of the community. Organisations may be asked – by stakeholders or regulators – about how they are addressing some of these broader community issues. Reporting frameworks, such as the Global Reporting Initiative (GRI), and social indices like FTSE4Good are becoming more mainstream as stakeholders demand greater transparency on an organisation's social impacts. Often these issues are beyond the organisation's direct control but still require oversight and influence in the eyes of the community.

The organisation, Partnership on AI, has been established to study and formulate best practices on AI technologies, advance the public's understanding of AI, and serve as an open platform for discussion and engagement about AI and its influences on people and society. For further information, go to <https://partnershiponai.org/>

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

ALGORITHMS

Algorithms in their simplest form, are a set of instructions to solve a problem or complete a task. They form the basis of most AI we see in everyday platforms such as Facebook and Netflix. Data is collected and sorted, and the algorithms then make decisions through an iterative process of validation and verification from internal and external sources. The outcomes of these complex algorithms inform decision-making in the organisation or buyers of the information.

One example is IBM Watson® AI – a learning platform using many algorithms and processes that takes in various forms of public and private information, arriving at outputs that help inform decision-making. The outcomes generated by Watson are calculated using a set of instructions and behavioural parameters, including psychological and mood-reading information, based on specific words or sentence structures used.

GOVERNANCE ISSUES ASSOCIATED WITH AUTOMATION AND AI

We are in an environment where directors must now govern for constant change rather than for managing change from one fixed state to another. With **foresight, insight and oversight** – the keystones of governance – directors must apply these lenses to all aspects of their organisation in the context of automation and AI.

Foresight must include consideration of automation and AI and the different risks and opportunities they present to your organisation. Anticipating the required changes within your organisation is critical. It may be as simple as knowing who can advise on the impact of technology disruption or as complex as considering how to redefine the very industry your company operates in. Bringing new technology and consumer scenarios – disrupting old thought patterns and ways of doing things – is imperative to test the sustainability of the existing business model. The past is no longer always a good predictor of the future. As AI is adopted within the business world and in our private lives, successful organisations will be open-minded and committed to staying ahead of, or at least at pace with the pack, and maintaining public trust.

Insight takes the form of truly understanding the wide range of risks and opportunities specific to your industry and your organisation. What value can you bring to the discussion about the impacts of these changes on you and your customers? Directors need to inform themselves and provide relevant challenges and feedback to management when developing and embedding innovation and technology solutions into their business.

As a board member, consider the following examples. What are some of the challenging questions you would ask to determine your organisation's risks, opportunities, and strategies?

- Example 1 – The CEO of your organisation comes to your board with a proposal for a new form of technology that would allow you to collect personal data from your customers (through wearable clothes that gather physiological data) and use automation and AI to conduct processing and analyses. What are the risks associated with this from a privacy perspective? What are your responsibilities with the data? How could you use the information to serve your customers better? How could you use the information to generate additional forms of revenue? Are there any ethical issues (for example, selling this data to health insurers) that may impact individual customer health insurance premiums? What if the information is inaccurate? Who is liable?
- Example 2 – Your CEO comes to the board with a proposal to introduce AI that can analyse data on your truck drivers. Heart rates, driving styles, rest breaks, and other data could help improve your workers' safety and the efficiency of your deliveries, perhaps even shape incentive and accountability frameworks. How might this impact employee relations? How could this data reduce or improve profitability (e.g. reducing insurance premiums for trucks) or reshape your business model entirely? What are the privacy and health obligations regarding the drivers' data you would hold?

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

Broadly, directors need to consider what information they need to be able to challenge and test management's assumptions constructively. In this context, directors need to seek tension in the business that pushes the organisation into more innovative and lateral thinking. If you are not generating a little tension, you may not be getting close enough to the value creation needed to succeed in a new operating environment.

The **oversight** role for automation and AI is largely the same as for any other area of governance. Just as the board needs to develop relevant KPIs for performance (for example, concerning financial oversight), the board also needs to develop relevant KPIs that will enable oversight of innovation and technology adoption success. The board should consider any risk thresholds that might apply to innovation and 'planned' disruption to its business. These thresholds include having clarity over when to walk away from an automation or AI project that is not performing as planned.

Oversight from external bodies may also increase in areas of automation and AI. For example, governments will be increasingly expected to consider regulation of AI usage based on ethical concerns (such as systemic biases, fairness or privacy issues) or to incentivise the decommissioning of redundant ways of doing business due to community demands for change.

Amongst all these changes, there is also a role for **AI to assist the board** in their oversight role. For example, it will not be long until 'Siri' (or similar) is available to answer questions, and you can ask: 'Siri, have we complied with our reporting obligations this quarter?'

AI systems are fallible as they are built and run by humans. As a result, they will likely continue to make mistakes, and directors will need to ensure that the organisation considers the risks and appropriate safeguards. Further, directors must ensure they remain correctly informed of the company's financial position (beyond merely asking a 'bot') to ensure they comply with their legal duties (see Chapter 1.1).

In some cases, it may not be crucial to know how and why an AI system makes a decision. However, in other cases, it may be critical, for example, to decide what medications should be provided to a patient or what custodial sentence should be imposed for a conviction.

Automation and AI should be fully understood, regularly retrained and tested and continually updated and managed. To achieve this, some leading global organisations have even included bots in their organisational charts, effectively giving business line-managers responsibility for their oversight and performance management just as they would their human direct reports (although they're less likely to get a year-end bonus).

GOVERNANCE IN REGULATORY UNCERTAINTY

Regulation in a changing environment presents a challenge for businesses. Often businesses like a certainty to predict and control risk, and a stable regulatory environment can be beneficial. However, with ongoing rapid advancements in automation and AI, regulation can lag significantly behind 'cutting-edge' use cases.

Often, we see that existing regulation is updated to keep pace with community changes. For example, regulatory change can be in response to specific events, lobbying designed to incentivise investment, deter misconduct, or protect rights that reflect community standards and expectations. But unfortunately, the pace of technology change far exceeds the rate of change in any regulatory and governance frameworks. In addition, the global nature of the digital economy during this fourth industrial revolution means that reaching consensus or consistency in regulations can take even longer.

So how do directors govern in the face of: (i) uncertainty over the pace and extent of future regulation; (ii) multiple jurisdictions and cross-border differences in regulation; and (iii) inadequate regulation or regulatory protections that do not keep pace with the technological issues?

In the absence of up-to-date regulation, a more agile and proactive approach to governance is required – and is likely to become more and more essential. Anticipating technology changes, anticipating regulation, anticipating (or leading) sector and industry codes of conduct – and changing strategies in response – may be required to maintain a competitive edge.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

• GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

APPENDICES

CONTACT US

THE ROLE OF THE BOARD

The board has responsibility for creating a vision of the organisation's future based on foresight that considers a range of scenarios.

In the context of a more automated and artificially intelligent world of customer interactions, manufacturing processes and data analytics, directors need to:

- be curious and informed, constantly asking, 'What is the new tech trend?'
- understand how automation and AI technologies (no matter how far-fetched they may seem in today's terms) will impact the business in the short, medium and longer term
- put existing and future strategies into context – whilst change is difficult or may not seem necessary in today's terms, what are the risks of *not* adapting to these changes?
- expect the unexpected – even the most unlikely scenarios can come to fruition (who would have thought that driverless cars would be possible so soon?)
- encourage innovation and be prepared to fail at times (within defined risk thresholds)
- look holistically at the organisation's strategic assets, recognising that they may no longer be physical assets but focused more on customer experience
- proactively recruit board members who can constructively question and challenge the organisation's strategies.

Useful resources

- Partnership on AI, <https://partnershiponai.org/>
- Gartner research, <https://www.gartner.com/en>

For further information please contact:



Dhawal Jaggi

**Partner – AI Foundations
and Transformation Lead
KPMG Australia
dhawaljaggi@kpmg.com.au**

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

• GLOSSARY

APPENDICES

CONTACT US

Glossary

AASB	Australian Accounting Standards Board	CCPA	California Consumer Privacy Act
ACCC	Australian Competition and Consumer Commission	CDR	Consumer Data Right
ACNC	Australian Charities and Not For Profits Commission	CEO	Chief Executive Officer
ACSC	Australian Cyber Security Centre	CFO	Chief Financial Officer
ACSI	Australian Council of Superannuation Investors	CIO	Chief Information Officer
ADI	Authorised Deposit-Taking Institutions	CISO	Chief Information Security Officer
AFS	Australian Financial Services	CPS	Consolidating Prudential Standards
AGM	Annual General Meeting	COP	Conference of Parties
AI	Artificial Intelligence	CPA	Certified Public Accountant
AIATSIS	Australian Institute of Aboriginal and Torres Strait Islander Studies	CRO	Chief Risk Officer
AIC	Australian Investment Council	CR	Corporate Responsibility
AICD	Australian Institute of Company Directors	CSF	Crowd-Sourced Funding
APP	Australian Privacy Principles	D&O	Directors and Officers
APRA	Australian Prudential Regulation Authority	DoA	Delegation of Authority
ASIC	Australian Securities and Investment Commission	EER	Extended External Reporting
ASIO	Australian Security Intelligence Organisation	EFLIC	Eligible foreign life insurance organisations
ASX	Australian Securities Exchange	ERM	Enterprise Risk Management
ATO	Australian Taxation Office	ESG	Environmental, Social and Governance
AUASB	Auditing and Assurance Standards Board	FRC	Financial Reporting Council
BRC	Board Risk Committee	FTE	Full Time Equivalent
CA ANZ	Chartered Accountants Australia and New Zealand	GAAP	Generally Accepted Accounting Principles
CalPERS	California Public Employees Retirement System	GAPP	Generally Accepted Privacy Principles
CAMAC	Corporations and Markets Advisory Committee	GIA	Governance Institute of Australia
CATSI Act	The Corporations (Aboriginal and Torres Strait Islander) Act 2006	GDPR	General Data Protection Regulation

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

• GLOSSARY

APPENDICES

CONTACT US

GFC	Global Financial Crisis	PE	Private Equity
GPFS	General Purpose Financial Statements	PEC	Private Equity Committee
GRC	Governance, Risk and Compliance	PPG	Prudential Practice Guide
GRI	Global Reporting Initiative	PRI	Principles for Responsible Investment
GST	Goods and Services Tax	RAPs	Reconciliation Action Plans
HSEC	Health, Safety, Environment and Community Committee	RBA	Reserve Bank of Australia
HSR	Health and Safety Representative	ROI	Return on Investment
IASB	International Accounting Standards Board	RPA	Robotic Process Automation
ICGN	International Corporate Governance Network's	RSE	Registerable Superannuation Entities
IFRS	International Financial Reporting Standards	SASB	Sustainability Accounting Standards Board
IIA	Institute of Internal Auditors	SEC	US Securities and Exchange Commission
IMF	International Monetary Fund	SGC	Super Guarantee Charge
IOT	Internet of Things	SLACI Bill	Security Legislation Amendment (Critical Infrastructure) Bill 2021
ISO	International Organization for Standardisation	SLACIP Bill	Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022
KMP	Key Management Personnel	SMSF	Self-Managed Superannuation Fund
KPI	Key Performance Indicators	SOCI	Security of Critical Infrastructure Act
LIT	Lost Injury Time	SOX	Sarbanes-Oxley Act
LPI	Leading Performance Indicator	SPFS	Special Purpose Financial Statements
M&As	Memorandum and Articles of Association	TCFD	Task Force on Climate-related Financial Disclosures
MD	Managing Director	TNFD	Task Force on Nature-related Financial Disclosures
NDB	Notifiable Data Breach	TP	Transfer Pricing
NIST	National Institute of Science and Technology	TrueTCO	True Total Cost of Ownership
NFP	Not for Profit	TTC	Tax Transparency Code
OAIC	Office of the Australian Information Commissioner	UN-FCCC	United Nations Framework Convention on Climate Change
OECD	Organisation for Economic Cooperation and Development	WEF	World Economic Forum
ORIC	Office of the Registrar of Indigenous Corporations	WHS	Workplace Health and Safety
PAYG	Pay as You Go		
PCBU	Person Conducting a Business or Undertaking		

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

Appendix 1: Board Charter

The purpose of a board charter is to describe the board's terms of reference and outline the board's approach to important governance practices.

Research into board charters of Australia's top 50 listed companies indicates that charters can cover a broad range of matters, including those in the box below:

Matters which may be found in a board charter

– Board role descriptions	– Access to management
– Role of chairman	– Code of conduct
– Role of the committee chairmen	– Corporate social responsibility/sustainability
– Role of the company secretary	– Political donations
– Role of managing director/CEO	– Compliance system
– Director letter of appointment	– Policies and procedures
– Directors' induction and education	– Board's role in crisis management
– Tenure	– Integrity of financial reporting
– Board committees	– CEO and CFO assurance
– Conflicts of interest	– Annual report to shareholders
– Indemnities and insurance	– Reporting to stakeholders
– Deed of indemnity, insurance and access	– Annual general meeting
– Directors' and officers' insurance	– Board and individual directors' performance assessment
– Access to board papers	– Review of CEO performance
– Access to independent professional advice	– Director remuneration
– Strategic direction and oversight	– Quorum

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

Appendix 2: Annual Agenda

The board and annual agenda should be designed as a practical work plan where the board's staple business items are allocated to a particular meeting. The example annual agenda attached is one approach to the categorisation of business items and their allocation to specific meetings. In this example, it is assumed there will be 12 meetings of the board including an annual strategy day. An underlying objective of the annual agenda is to achieve balance in the board's workload through the year and ensure all board responsibilities are attended to.

The items of business have been categorised as follows:

- matters that the board has resolved for its decision (reserved authorities)
- matters which have been delegated (e.g. to the CEO or a board committee) (delegated authorities)
- matters that are purely for information and do not require a board decision (reporting)
- procedural matters that may arise at any or every board meeting (matters that may be applicable to all meetings).

The matters listed in the annual agenda and the scheduling of such matters will vary from company to company. Each board should identify the core matters for inclusion in the annual agenda. As well as the anticipated board business, there will be other matters which arise that require the board's attention such as a merger or acquisition or major capital expenditure. An annual agenda may be set out in many different ways. A different format is provided in [Appendix 5 Audit committee and annual agenda](#).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

Reserved authorities	Delegated authorities	Reporting	Matters that may be applicable to all meetings
Meeting 1 – Board charter – Annual agenda – Retained authorities – Delegated authorities – Chairman, individual director and committee roles – Company secretary's role – Advisory boards – Full-year or interim financial reporting – CEO's position description and goal setting	– Investor relations strategy – Management delegations, accountability and approval levels – Board and management information system – Strategic plan (actions and accountabilities)	– Regulatory and compliance report – CEO/CFO report	– Conflict and disclosure of interests – Litigation and non-compliance issues – Insider trading – Share trading – Continuous disclosure – Access to company records – Meeting agenda/ papers/ preparation/procedures/ decision-making processes – Independent professional advice

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

	Reserved authorities	Delegated authorities	Reporting	Matters that may be applicable to all meetings
Meeting 2	– Board and committee succession planning – Risk appetite and risk management policy	– Risk management strategy – Risk profile and assessment – Management accountability for risk – Internal control environment	– Audit committee report – CEO/CFO report – Major project reports – Risk management report	– Protocols for board/ management interaction between board/ committee meetings – Decision-making outside the boardroom (circular resolutions) – Board minutes – In camera minutes – Board member induction and education
Meeting 3	– CEO succession planning – Board training plan – Corporate planning and budgeting	– Reporting and communications strategy – Review of key policies and procedures	– Investor relations report – Remuneration committee report – CEO/CFO report	
Meeting 4	– Director appointments/ re-election – Director remuneration policy – Non-executive director remuneration – Director independence – Review of constitution	– Code of conduct – OH&S plan – Corporate budgeting and planning	– Regulatory and compliance report – CEO/CFO report	
Meeting 5	– Directors' and officers' indemnity and insurance – Internal audit plan – External audit plan	– Whistleblower policy – IS strategy/policy – Director induction program	– Audit committee report – CEO/CFO report – Major project reports – Risk management report – Analyst and institutional presentations	

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

Appendix 3: Audit Committee Charter

PURPOSE

The audit committee (the committee), appointed by the board of directors (the board), assists the board to fulfil its oversight responsibilities relating to:

- the preparation and integrity of the company's financial accounts and statements
- internal controls, policies and procedures that the company uses to identify and manage business risks
- qualifications, independence, engagement, fees and performance of the external auditor
- the external auditor's annual audit of the financial statements
- the resources, performance and scope of work of the internal audit function
- company compliance with legal, regulatory requirements and compliance policies.

Effective corporate governance depends on the active and collaborative participation of the committee, board of directors, external auditors, internal auditors, other assurance providers and management. Ensuring that this collaboration occurs effectively and efficiently is fundamental to the committee's success.

The existence of the committee does not diminish the board's responsibility to ensure the integrity of the financial reporting.

AUTHORITY

The board has authorised the committee, within the scope of its duties and responsibilities set out in this charter, to:

- perform the activities required to address its responsibilities and make recommendations to the board
- resolve any disagreement between management and the external auditor, with areas of significant disagreement being advised to the board
- select, engage and approve the fees (within operational limits) for professional advisers that the committee may require to carry out its duties
- subject to the agreed protocol:
 - require the attendance of any company manager or staff member at meetings, as appropriate
 - have unrestricted access to management, employees and information it considers relevant to its responsibilities under this charter.

MEMBERSHIP

The board chairman is responsible for nominating committee members for approval by the board.

The committee will comprise at least [insert number] members, all of whom should be independent (as defined in the board charter) non-executive directors.

The committee members must be 'financially literate' (i.e. able to read and understand financial statements and challenge information presented in committee meetings).

At least one committee member must have 'accounting or related financial expertise' and at least one member must have relevant industry experience.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

Committee member appointments are for an initial term of [insert number] years and the appointment is reviewed annually, or earlier, if circumstances dictate.

Committee member rotation is encouraged. Wherever possible, the board also ensures that changes in committee membership are staggered to maintain continuity.

The company secretary or their designate is the committee secretary.

CHAIR

The board chair is responsible for nominating the committee chair for approval by the board.

The committee chair must be an independent, non-executive director and not the chair of the board.

Should the committee chair be absent from a meeting, the committee members present must appoint a chair for that particular meeting, who should not be the chair of the board.

EDUCATION

The company will assist the committee in maintaining appropriate financial literacy, the company is responsible for providing new members with an appropriate induction program and educational opportunities, and the full committee with educational resources relating to accounting principles and procedures, current accounting topics pertinent to the company, and other resources, as reasonable requested by the committee.

MEETINGS

The committee must meet at least [insert number] times per year. If a member is unable to be physically present, they may participate by video or teleconference.

A notice of each meeting, with relevant supporting agenda papers, confirming the date, time and venue is to be forwarded to each committee member (with a copy to all directors) at least 5 working days before each meeting.

The committee chair, the board chair or any other committee member may call a meeting of the committee. The external auditor or internal auditor may request the committee chair or a committee member to call a meeting. The committee chair may waive the 5 working days notice period if agreed by all members.

The committee chair may invite any person or persons (other than duly appointed members) to attend meetings of the committee, but not necessarily for the full duration of the meeting, a standing invitation shall be issued to:

- other directors
- the CEO
- the CFO
- the internal and external auditors
- the compliance manager and other relevant members of management.

[Insert number] members will constitute a quorum.

The committee chair is not entitled to a second or casting vote.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

MINUTES

The committee secretary or delegate must prepare the minutes of the committee meeting within 7 working days. After the committee chair has given preliminary approval, the draft minutes are circulated to all committee members and the other board directors.

The minutes of the meetings must be confirmed and signed at the next committee meeting.

COMMUNICATION

The committee is expected to maintain free and open communication with the external auditor, the internal auditor and management.

DUTIES AND RESPONSIBILITIES

In assisting the board to fulfil its responsibilities, the duties of the committee are as follows.

Assessment of financial information

Review any significant accounting and reporting issues, including professional and regulatory announcements, and understand their effect on the company's financial statements.

Review all published half-year and annual financial statements of the company, which require the approval of the board, based on the recommendation of the committee, and hold discussions regarding the financial statements with the external auditor and management before submission to the board.

The committee will pay specific attention to:

- the consistency of accounting policies and appropriate adoption of any new accounting standards
- considering the need for, appropriateness of and correct disclosure of, any changes made to the company's accounting policies
- the treatment and disclosure of complex or unusual transactions, including off-balance sheet structures

- significant judgements made by management in preparing the financial statements, including any significant accounting estimates
- the going-concern assumptions
- review, at least annually, the written attestations provided by the CEO and CFO for Australian reporting purposes that:
 - the company's financial records have been properly maintained
 - the company's financial statements and notes present a true and fair view, in all material respects, of the company's financial condition, and are in accordance with relevant accounting standards
 - the financial statements are founded on a sound system of risk management and internal compliance and control, and that the system is operating effectively in all material respects in relation to financial reporting risk
 - the company's risk management and internal control and compliance systems are operating efficiently and effectively in respect to its material business risks.

External auditors

Recommend to the board the appointment, evaluation and removal of the external auditors.

Review and approve the external auditors' proposed audit plan and audit approach, including materiality levels.

Review and agree on the terms of engagement and the audit fees for the external auditors prior to the commencement of each audit.

Review the independence and objectivity of the external auditors and their compliance with all relevant independence requirements including:

- financial interests in clients and other business relationships
- employment and other personal relationships
- the level of non-audit services provided
- the rotation of audit partners
- limitations on external audit partner providing services other than audit, review or attestation.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

Understand any material alternative treatment of financial information that has been discussed with management, including their ramifications, together with the treatment preferred by the external auditor.

Discuss the appropriateness of accounting policies, estimates and judgements.

Review the external auditor's summary management report, detailing the results and significant findings from the audit and management responses.

Meet regularly with the external auditor, without management present.

Resolve any disagreements between management and external auditors in the financial reporting and advise any significant issue to the board.

Review and approve the external auditor's process for the rotation and succession of audit and review partners, including their approach to managing the transition.

Obtain from the external auditors and review the independence declaration required under the Corporations Act.

Internal auditors (if any)

Approve the appointment, remuneration and removal of the head of internal audit.

Review the internal audit charter to ensure the appropriate organisational structure, authority, access and reporting arrangements are in place. Ensure appropriate resourcing of the internal audit function.

Approve and review progress against the internal audit work plan:

- review the internal audit coverage and annual work plan, and monitor progress of the work plan
- advise the board on the adequacy of internal audit resources to carry out its responsibilities, including completion of the approved internal audit plan
- oversee the co-ordination of audit programs conducted by internal and external audit respectively
- review significant internal audit reports and findings.

Review progress on management actions. Monitor progress against the annual work plan, including any significant changes to it, any difficulties or restrictions on the scope of activities and any significant disagreements with management.

Discuss issues with internal audit in the absence of management.

Consider the major findings of the internal audit reports and review management's response in terms of content and timeliness. Monitor management's implementation of internal audit recommendations. Periodically review the performance of internal audit.

Risk management and internal controls

Approve the company's risk management policy and oversee the risk management system, including the risk management function and its resourcing.

Approve and monitor the company's risk profile developed by management, covering the principal enterprise-wide risks, including strategic, operational, legal and financial.

Review the operational effectiveness of the policies and procedures relating to risk and the company's internal control environment.

Review management evaluation of the effectiveness of internal controls.

Review the effectiveness of the company's insurance activities.

Ensure executive remuneration risk and controls are linked to the overall risk profile.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

Compliance

Review the effectiveness of the company's approach to achieving compliance with laws, regulations, industry codes and company policies.

Review compliance with the company's values and related behaviours and the code of conduct. Review and monitor the effectiveness of policies, procedures and processes for complying with continuous disclosure requirements.

Obtain regular updates from management, legal counsel and the company secretary regarding compliance matters that may have a material impact on the company's activities. Review any correspondence from regulatory bodies regarding significant issues.

Other responsibilities

Ensure that there is a process in place for the board chair and committee chair to be immediately informed of any issue of significant non-compliance or litigation. Oversee the process for the receipt, retention and treatment of information received from the internal whistleblower policy and procedures, and also from external complainants regarding matters relating to audit, the financial statements, internal controls or possible fraud.

Review any fraud reports. Review and discuss any reports concern any breach of fiduciary duty. Hold regular executive sessions with the CEO, CFO and other senior management to discuss private matters with the committee.

Act as a forum for communication between the board and senior management and internal and external audit. Review the effectiveness and level of cooperation between management, the internal auditor (if any), the risk management function (if any) and the external auditors. Review reports to the shareholders on the role and responsibilities of the committee. Conduct special investigations (if required). Perform any other duty of undertaking that the board may request from time to time.

Review, for potential conflict of interest situations, and pre-approve related party transactions on an ongoing basis.

REPORTING

In addition to providing the board with a copy of the agenda, committee papers and minutes of its meetings, the committee will ensure that:

- the committee chair reports to the board on committee meetings, regarding all relevant matters and appropriate recommendations, in a written report (with supporting material) for noting or approval by the board
- the committee addresses any other reporting responsibilities.

REVIEWS

To ensure that the committee is fulfilling its stewardship duties to the board, the committee will:

- review, at least annually, the committee charter and recommend to the board any appropriate amendments for approval
- review the annual agenda incorporating any changes in the charter
- conduct an annual assessment of its performance against its charter duties and responsibilities and provide a report of the findings to the board
- conduct an annual assessment of each committee member (the committee chair should provide a report of the findings to the board chair).

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

Appendix 4: Audit Committee Induction Framework

Over the last few years the responsibilities of audit committees have increased significantly. It is no longer sufficient for audit committee members to have only a rudimentary knowledge of financial and regulatory matters. Committees cannot provide meaningful protection for shareholders unless their committee members are in a position to challenge management. To do this effectively, they must have the skills, knowledge and expertise, and be supported by access to independent advisers.

A formal induction program for new committee members is essential. A comprehensive committee induction program could include an information package, training sessions and meetings with key executive. The following outlines suggested inclusions in an induction framework.

INFORMATION PACKAGE

An information package could include:

- committee charter
- committee annual agenda
- committee papers and minutes for the previous 12 months
- outline of the resources used by the committee to undertake its duties
- external auditor relationship
- accounting policies and approved practices
- regulatory and compliance framework for the company's business
- risk management policies
- risk management and control framework
- internal auditor's work plan
- details of the compliance framework, together with background on the key compliance obligations, both internal and external
- last annual report to the board on how the committee has discharged its duties.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

TRAINING SESSIONS

Training sessions could be facilitated to guide audit committee members on:

- protocols
- effective meetings
- roles and accountabilities
- conflict of interest
- financial report review
- internal audit planning
- risk reporting review and attestation
- internal audit report review
- compliance reporting review
- external audit reporting.

MEETINGS

Meetings to discuss the committee charter, how the committee operates, the main business and financial dynamics and other matters of significant could be held with the:

- committee chair
- CEO
- CFO
- internal auditor
- compliance officer
- company secretary and general counsel
- external auditor.

In addition, it may be useful to schedule discussions with other senior management regarding key operations and hold a follow-up meeting with the committee chair to discuss any issues arising from the induction program.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

Appendix 5: Audit Committee Annual Agenda

This example annual agenda is linked to the example audit committee charter. In this example there are five scheduled committee meetings planned for the year.

Scheduled meetings					
	Dec	Feb	Mar	Jul	Sept
Foundation					
Review audit committee charter and annual agenda					
Assess committee's independence, financial literacy, skills and experience					
Determine number of meetings for forthcoming financial year					
Committee chairman to determine meeting agenda and required attendees, including management and assurance providers					
Enhance financial literacy – update on current financial events					
Review of ongoing audit committee member education plans					
Conduct an assessment of the committee's performance against its charter and provide a report to the board					
Conduct an assessment of the individual member's performance					
Consider committee member rotation and succession planning					

 Recommended timing

 As required

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

	Dec	Feb	Mar	Jul	Sept
Assessment of financial information					
Review significant accounting and reporting issues					
Review financial matter affecting the half year					
Review and approve half year financial statements					
Review financial matters affecting the year end					
Review and approve annual financial statements					
Review attestations of the CEO and CFO for Australian reporting					
Review with management its evaluation of internal control structure and procedures for financial reporting, including any significant deficiencies or material weaknesses					
Scheduled meetings					
	Dec	Feb	Mar	Jul	Sept
Annually review and discuss with management and the external auditors, management's assessment of the effectiveness of internal control structure and procedures for financial reporting					
Review and discuss any reports concerning evidence of material violation or breaches of fiduciary duty					
Review and discuss any reports submitted by the external auditor detailing any instances of fraud or possible illegal acts on the part of senior management					
Review process, policies and procedures for continuous disclosure obligations					
Review conflicts of interest and related party transactions					
External auditors					
Recommend appointment, evaluation and removal of the external auditors					
Review audit plan and scope of audit work and any changes thereto					
Recommend terms of engagement and audit fees					
Consider policy in relation to non-audit services					

 Recommended timing  As required

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

	Dec	Feb	Mar	Jul	Sept
Review and pre-approve non-audit services					
Consider objectivity/independence and obtain independence declaration from external auditor					
Review external auditors' report and findings and progress on management actions					
Discuss implications of any significant changes in accounting standards					
Discuss appropriateness of accounting policies, estimates and judgements					
Discuss external auditors' view on control environment, including fraud and risk management					
Resolve any disagreement between management and the external auditor in the financial reporting and report any significant issues to the board					
Discuss issues with auditor in the absence of management					
Ongoing communication (written/oral) between the external auditor with the committee					
Review report from external auditor on quality control procedures					
Review the external auditors process for rotation and approach for managing transition					
Internal auditors					
Approve appointment and review performance					
Review internal audit charter					
Review internal audit plan and any changes required to the plan including any resource issues					
Review progress against the audit plan					
Review significant internal audit reports and findings					
Review progress on management actions					
Discuss issues with the internal auditor in the absence of management					
Review the performance of internal audit ¹ , including organisational structure, qualifications and independence.					
Recommended timing			As required		

 Recommended timing  As required

¹ Undertaken by an external party periodically, e.g. every 2 to 3 years.

FOREWORD

THE ROLE OF BOARDS AND DIRECTORS

1. Directors' Legal Duties
2. Governance Roles
3. Government
4. Not-For-Profit Organisations
5. Proprietary Limited Companies
6. Indigenous Culture

GOVERNANCE ACCOUNTABILITY

7. Accountability to Shareholders
8. Stakeholder Engagement

GOVERNANCE LEADERSHIP

9. Structuring an Effective Board
10. Company Leadership
11. Board Committees
12. Investment Management
13. Productive Meetings
14. Strategy and Planning
15. Receiving Assurance
16. Tax Governance and Transparency
17. Risk Management

GOVERNANCE OVERSIGHT

18. Environmental, Social and Governance (ESG)
19. Safeguarding of Vulnerable People
20. Private Equity
21. Health, Safety and Wellbeing
22. Culture and Conduct
23. Cybersecurity
24. Data Privacy and Personal Information
25. Human Rights and Modern Slavery
26. Automation and AI

GLOSSARY

• APPENDICES

CONTACT US

	Dec	Feb	Mar	Jul	Sept
Risk management and internal controls					
Review risk management policy and risk management system					
Review risk profile					
Review internal controls and report to the board					
Review operational effectiveness of risk policies and procedures and internal control environment					
Review the effectiveness of the company's insurance activities					
Ensure effective remuneration risk and controls are linked to the overall risk profile					
Compliance					
Review legal and regulatory matters that may have a material impact on the company					
Review compliance report from management, and correspondence (if any) from regulatory bodies					
Review any correspondence from regulatory bodies					
Review compliance with company values and related behaviours, and the code of conduct					
Review compliance with continuous disclosure requirements					
Other responsibilities					
Review whistleblowing arrangements and reports					
Review fraud report					
Hold regular executive sessions with senior management					
Review level of cooperation between management, internal auditor and external auditor					
Review report to the shareholders on the role and responsibility of the committee					
Conduct special investigations and perform other activities, as appropriate					
Reporting					
Maintain minutes and report to the board					

 Recommended timing  As required



Contact us



Martin Sheppard
National Chairman

KPMG Australia

E: msheppard1@kpmg.com.au



Caron Sugars
**Lead Partner,
Board Advisory Services**

KPMG Australia

E: ccobargsugars@kpmg.com.au

ABOUT THE KPMG BOARD LEADERSHIP CENTRE

KPMG's Board Leadership Centre is a global program connecting and supporting non-executive directors in facing today's challenges, anticipating emerging threats and harnessing new opportunities.

Members gain access to exclusive tools and resources as well as an extensive network of other non-executive directors to help navigate the ever-changing demands of society and the business world.

Directors have the opportunity to trade insights, share ideas and support each other in tackling today's boardroom issues.



Connor Rolston
**Program Leader,
Board Leadership Centre**

KPMG Australia

E: crolston1@kpmg.com.au

[KPMG.com.au](https://www.kpmg.com.au)



The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

©2025 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Liability limited by a scheme approved under Professional Standards Legislation.

August 2025. 1633146046BLC.