

INTERNAL AUDIT IN FOCUS FY23

In an increasingly volatile and disrupted world, Chief Audit Executives (CAEs) and Internal Audit teams must remain agile in the context of a rapidly changing risk landscape. Drawing from KPMG's Australian publication Keeping us up at night – the big issues facing business leaders in 2022¹ our recommended key areas of focus for FY23 planning tailored for Australia are outlined in this report.

¹ Keeping us up at night (assets.kpmg)

Internal Audit in Focus FY23

Economic Risks (including geopolitical)

The strength of recovery in the global economy, spending patterns switching towards goods and away from services, and Covid-19-related disruptions in logistics networks have generated significant inflationary pressures. Economic recovery is very visible in the labour market, with the unemployment rate currently just 4.2%. Limited spare capacity is putting upward pressure on wages, as firms compete to secure the talent they need. With the economy closing in on a full recovery from the pandemic, the RBA is likely to begin raising interest rates in the second half of the year.

When it comes to the ongoing situation in Ukraine it is important to consider various commercial, logistical, legal and broader geological impacts (including the complex sanctions regime). From cutting off the supply of key inputs, to financial market spikes caused by the freezing of global assets, to threatening the distribution of key energy stocks – sanctions of all kind are creating new day-to-day risks in the commercial agenda of global organisations.

4.2%
UNEMPLOYMENT RATE

INTERNAL AUDIT RESPONSE

Consider how the first and second lines are identifying and assessing where these risks and pressures are likely to impact the organisation. Internal audit should also review third party suppliers exposed to economic shifts, and more broadly consider organisational capital planning and capital management, net interest margins, credit/default risk and debt recovery, claims management and businesses cases for future investment.

Internal Audit can also play a role in identifying and assessing potential immediate gaps or control weaknesses in relation to compliance with the current international sanctions regime and ensuring there is a robust framework which includes appropriate risk mitigation measures that can be applied on an ongoing basis to help remain compliant.



ESG (Environmental, Social and Governance)

Whilst specific ESG reporting is not yet mandatory in Australia, there is a rapid movement towards this. For example, in November 2021 APRA produced a Prudential Practice Guide CPG229 Climate Change Financial Risk, as a framework to assist in managing climate risks. ASIC is also encouraging companies to ensure they have appropriate governance structures to respond to ESG, and to provide reliable and useful information on their ESG risks and opportunities. ASIC is encouraging the use of the framework from the Financial Stability Board's Taskforce for Climate Related Financial Disclosures (TCFD)².

Coupled with this, expectations are increasing from investors, regulators, shareholders, customers and employees for organisations to operate with an ESG lens on all that they do. Internal Audit should play a key role in supporting all organisations to effectively manage ESG risk.

INTERNAL AUDIT RESPONSE

For organisations at an early stage of their ESG journey, Internal Audit should provide advisory support in understanding ESG risk, supporting the design and development of robust governance frameworks and control environments.

For organisations further progressed on their ESG journey, Internal Audit should provide assurance over relevant governance frameworks, organisational strategies, commitments, policies and plans, including the integrity of ESG reporting. Compliance with ESG risk management and relevant legislative requirements should also be considered.

² Managing climate risk for directors | ASIC - Australian Securities and Investments Commission

Talent Management & Wellbeing

The availability and retention of talent remains a key risk post the Covid-19 pandemic, together with the legacy of associated border closures. Employee wellbeing remains severely impacted, increasing the risk of loss of talent, fatigue and associated productivity impacts, together with the erosion of purpose and culture.

INTERNAL AUDIT RESPONSE

Assess the organisation's workforce and future skill demand planning, talent sourcing and talent retention strategies. These should include succession planning, capability management, remuneration benchmarking, wellbeing programs, and training and development.



Cyber Security

Remote working and the speed at which new technologies are adopted, coupled with global players increasingly using cyber disruption as a critical tool in their arsenal, means organisations must remain hyper vigilant to their cyber security risk. This accentuates the need for greater scrutiny of IT security and workforce awareness to malicious and non-malicious threats.

Further, the Security Legislation Amendment Bill 2020, coupled with the proposed Security Legislation Amendment (Critical infrastructure Protection) Bill 2022³, increased the range of organisations that now fall within the expanded definition of critical infrastructure assets. Additional cyber security obligations may need to be considered, including a risk management program, cyber incident reporting requirements, and information reporting.

INTERNAL AUDIT RESPONSE

Assess the veracity of controls to mitigate cyber security risk, and consider applying the NIST Cyber Security Framework⁴: Identify, protect, Detect, Respond and Recover. Example reviews could include Cyber Security governance, Identity Management, Awareness and Training, Security Assessment of Cyber Controls (including detection and response management), Cyber Security Health Check, Post Covid-19 New Ways of Working Review, Data Security practices, Incident Response and Recovery strategies.

Privacy & Data Protection

In a data-driven world powered by digitisation and remote working, regulators continue to increase their vigilance, and privacy and data protection risks continue to pose significant challenges to organisations. The imminent Australian Privacy Act reforms and expansions, coupled with the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Online privacy Bill) broaden privacy requirements and create a binding Online Privacy Code for social media and other online platforms.

INTERNAL AUDIT RESPONSE

Assess privacy and data protection controls related to how and what data is being collected, used, stored, secured, retained and disposed of, in line with regulatory requirements and industry-leading practices. Consider the management of organisational data which third party providers have access to. Perform a gap analysis against proposed legislative reforms, or a maturity assessment against the current Australian Privacy Principles⁵.

³ <https://www.legislation.gov.au/Details/C2021A00124>

⁴ Cybersecurity Framework | NIST

⁵ Australian Privacy Principles quick reference - Home (oaic.gov.au)

Fraud and Corruption

Many Australian organisations are now more vulnerable to fraud and corruption than they were before the pandemic and there is no indication the risk is subsiding. The increased vulnerability stems from extended periods of remote working, cost-cutting or diverting resources during the pandemic and seemingly an increase by employees to rationalise the act of committing fraud. 2021 also saw the release of the new Australian Standard 8001:2021 Fraud and Corruption Control which can assist management and Boards to benchmark their fraud and corruption control programs.

INTERNAL AUDIT RESPONSE

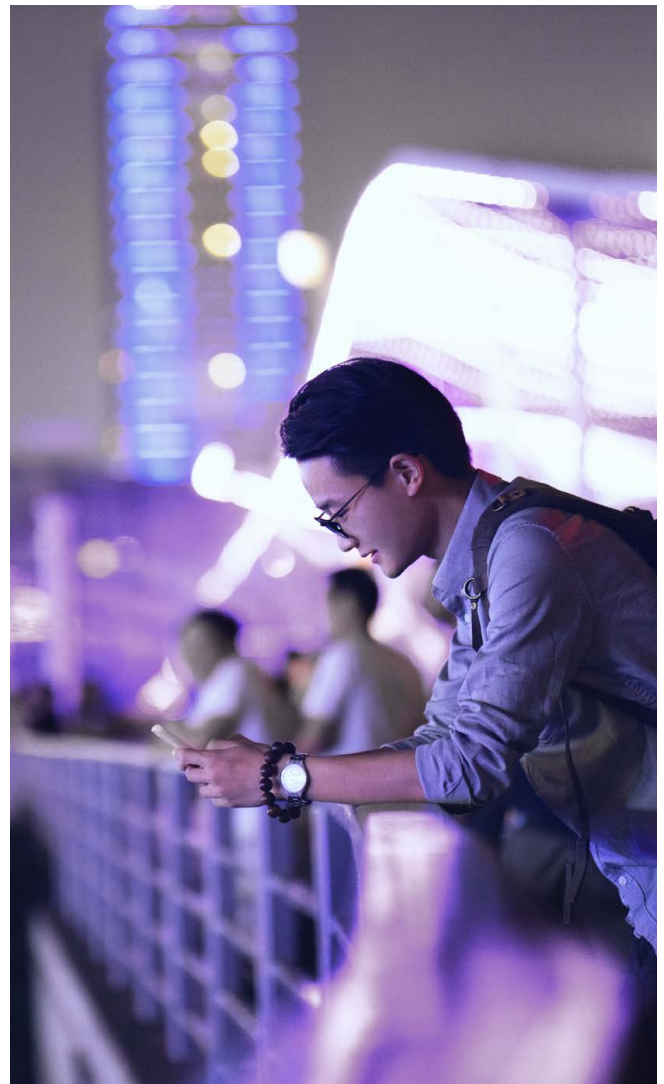
Assess the organisation's fraud and corruption control framework, fraud and corruption risk assessment procedures, together with fraud and corruption detection and response capability. As we emerge from the pandemic, consider fraud detection measures, including targeted data analytics to identify indicators of fraud and misconduct.

Third-Party Risk and Supply Chain

The pandemic continues to impose significant strain on global and domestic supply chains, from production delays and labour shortages, to continued shutdowns of major ports and associated shipping disruptions, increased commodity pricing, failure of third-party suppliers through to Modern Slavery and ESG considerations.

INTERNAL AUDIT RESPONSE

Assess scenario and contingency plans, including in supplier contracts and service continuity within these. Assess end to end procurement, with a specific focus on sourcing and third-party risk, and the distribution of that risk across suppliers. Review supply chain logistics and continuity processes, including third party cyber security risk management in their operating environments.



Digital disruption and new technologies

Digital disruption, transformation and adoption of new technology have accelerated through the pandemic, including AI, Predictive Analytics, Cognitive Computing and Robotic Process Automation. These bring new risks such as those relating to data and cloud storage, usage and privacy.

INTERNAL AUDIT RESPONSE

Assess the digitisation strategy and program together with associated risk management controls, provide assurance over specific digitisation projects, including AI design integrity, algorithm testing, exception management and remediation, change management controls, third party provider and software vendor management. Provide advice on governance and control frameworks to ensure long term AI and bot risks (post implementation) are monitored and mitigated.

Safeguarding of children and vulnerable people

In response to recent Royal Commissions and government enquiries, community expectations have rapidly increased in regard to the way organisations protect children and vulnerable people. Safeguarding governance and control structures can be preventative, participatory and detective, promoting an environment that keeps people free from abuse, exploitation and harm.

INTERNAL AUDIT RESPONSE

Focusing on where the risks to consumers lie, Internal Audit should assess preparedness and compliance against:

- Standards and/or legislation
- Commission recommendations
- Safeguarding policy
- Child safety or vulnerable people governance practices
- Safeguarding culture
- Incident management
- Complaints management

A review of a safeguards framework should consider preventive, participatory and detective safeguards.

Mergers and Acquisitions

Post Covid-19, a mergers and acquisitions boom accelerated through late 2021 with global mergers and acquisitions hitting new record highs. In Australia, this is also reflected in the speed of consolidation in the wealth management and superannuation industry. Mergers and acquisitions pose unique 'delivery' and 'delivered' risks during this period of rapid change and the need to realise the benefits of the transaction.

INTERNAL AUDIT RESPONSE

Develop an integrated merger risk assurance strategy and plan. This will allow informed decisions and awareness of the types of assurance the merger will obtain during its lifecycle, from real-time assurance through to 'go' / 'no-go' live assurance. A range of focus areas could include control due diligence of the target entity and remediation plans, governance and integration reviews, IT roadmap planning, supply chain consolidation and business case achievement.

Post Covid-19, a mergers and acquisitions boom accelerated through late 2021 with global mergers and acquisitions hitting new record highs.

Contact us

Rowena Craze

Partner, Governance Risk & Controls Advisory

E: rowenacraze@kpmg.com.au

Craig O'Hagan

Partner, Governance Risk & Controls Advisory

E: cohagan@kpmg.com.au

Phillip Sands

Partner, Governance Risk & Controls Advisory

E: pjsands@kpmg.com.au

Caron Sugars

Partner, Governance Risk & Controls Advisory

E: ccobargsugar@kpmg.com.au

Richard Cassidy

Partner, Governance Risk & Controls Advisory

E: rcassidy@kpmg.com.au

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).

©2022 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.

April 2022. 862286707AARC