

KPMG Australia CEO Review Report

1 OCTOBER 2026



Thursday, 1 October 2026

Mr John Sams
Chief Executive Officer
KPMG
Tower Two, Collins Square
727 Collins Street
Melbourne VIC 3008

Via email – jsams1@kpmg.com.au

Dear Mr Sams

R-051568 CEO Quality Review

We write to advise that the targeted quality review of your firm (**CEO Review**) directed by the Chief Executive Officer of Chartered Accountants Australia and New Zealand (**CA ANZ**) has been completed. We appreciate your assistance and co-operation throughout the CEO Review.

Approach

The Reviewer conducted the CEO Review in accordance with the scope set out in the Letter of Engagement. The review covered KPMG Australia and its related entities responsible for its Australian operations (**KPMG**) and the types of professional services identified in the agreed scope.

In particular, the Reviewer considered the design and implementation of KPMG's systems and processes for:

- storing and handling confidential information relating to audit clients, including processes for identifying, notifying and remediating instances of unauthorised use of confidential information; and
- promoting an ethical culture within the audit function and across the broader firm, including whistleblower protection policies and associated practices.

These areas were considered against the relevant requirements of APES 110 *Code of Ethics for Professional Accountants (including Independence Standards)*, ASQM 1 *Quality Management for Firms that Perform Audits or Reviews of Financial Reports and Other Financial Information, or Other Assurance or Related Services Engagements*, APES 320 *Quality Management for Firms that provide Non-Assurance Services* and APES 325 *Risk*

Management for Firms. This CEO Review results letter (**Results Letter**) and the enclosed document entitled Reviewer's Findings and Suggestions Report (**RFS Report**) have been prepared in accordance with our Letter of Engagement. For the avoidance of doubt, the confidentiality obligations outlined in the Letter of Engagement extend to this Results Letter and the RFS Report. For completeness, we note the firm has requested consent to provide a copy of this Results Letter and the RFS Report to a number of agencies and third parties, and to publish the documents to its website and CA ANZ has consented to such provision and publication.

The CEO Review was limited to the areas described in the Letter of Engagement and to the information and material provided by KPMG in relation to those areas. The reviewer has relied on the accuracy and completeness of any information and material they have received from your firm. The scope of the CEO Review does not include an independent verification of the accuracy and/or completeness of such information, except to the extent expressly described in the RFS Report. Accordingly, the conclusions in this Results Letter relate only to the matters within the agreed scope and should not be interpreted as an assessment of every element of KPMG's system of quality management.

In conducting the CEO Review, the reviewer has given your firm a reasonable opportunity to review and discuss the content of this Results Letter and the RFS Report and/or provide further material to address any issues identified by the reviewer. The reviewer has had regard to any further information provided in finalising this Results Letter and RFS Report.

The CEO Review is not an audit of the firm or files of any members of CA ANZ. By conducting the CEO Review, CA ANZ is not certifying or representing that the work done or the opinions given by a member or members generally, or for particular clients or on particular files, is correct or of a high or any particular standard. Further, the absence of a finding or suggestion should not be understood as confirmation that no deficiency, breach or other issue exists.

CA ANZ expressly disclaims all liability for any loss or damage (including on account of negligence) arising from any reliance upon the fact that CA ANZ has conducted the CEO Review, or upon any annual reports, overviews, reports on particular members or practices, or any other materials produced by CA ANZ regarding or in connection with the CEO Review or our Quality Review Program as a whole.

Documents which your firm has provided CA ANZ to conduct the CEO Review will be kept and destroyed in accordance with CA ANZ's internal policies and process relating to the retention of, and access to, review documentation.

The CEO Review and subsequently this Results Letter and RFS Report are not a substitute for your firm keeping itself informed as to and complying with all appropriate standards, rules and obligations. This review provides no guarantee as to whether the conduct of your firm is appropriate.

Results

We understand you have had the opportunity to discuss the reviewer's findings and suggestions in the RFS Report with them.

Based on the work performed within the agreed scope of the CEO Review, CA ANZ assesses that KPMG's systems and processes relating to the areas reviewed comply with the applicable mandatory requirements.

We would encourage you to consider implementation of the items included in the RFS Report as Better Practice Suggestions.

Conclusion

If you have any questions concerning this letter, please contact me. We would also be happy to receive any comments on the review process.

Yours sincerely

Caroline Karavias

Manager Quality Review

Quality Review Program

Reviewer's findings and suggestions report – 1 October 2026

Review Code: R-051568

This report has been prepared by the reviewer and details the reviewer's findings and suggestions for KPMG Australia (KPMG, the **Firm**) in relation to the targeted quality review directed by the Chief Executive Officer of Chartered Accountants Australia and New Zealand (**CA ANZ**) (**CEO Review**) under CA ANZ Regulation (CR2) 2.22(b).

1. Overall Reflections/Executive Summary

The targeted CEO Review was undertaken from July 2026 to October 2026.

No significant deficiencies were identified giving rise to findings in the two areas under review (refer Part 2) – with suggestions relating to the systems and processes for the storage and handling of confidential information of audit clients (confidential information) within the audit function as well as the systems and processes for promoting an ethical culture within the audit function, and across the organisation/firm more broadly including whistleblower protection policies and associated practices detailed in Part 9 below.

In relation to confidential information, the Firm has implemented a control environment encompassing governance, risk assessments, information security practices, incident management and compliance monitoring. Confidentiality obligations covering confidential information are embedded within policies, engagement terms and annual compliance processes, with accountability clearly assigned to partners and staff. Information security measures include access controls, secure client portals, data classification requirements, monitoring, data loss prevention activities and safeguards for KPMG Restricted information. Incident detection, escalation and investigation procedures support the identification and response to potential confidentiality breaches, including consideration of any client, regulatory or legal notification obligations that may arise. These arrangements are strengthened through ISO 27001 certification, structured risk assessment processes, internal audit activities and regular compliance reviews.

In relation to ethical culture, the Firm has implemented initiatives intended to embed ethical behaviour, accountability and public-interest obligations throughout the organisation. Ethical considerations are evident within the Firm's governance arrangements and strategy and operational activities and through initiatives such as the firmwide Ethics Champions Network. Ethical culture is overseen through monitoring,

surveys, reporting and review processes, with input from specialist internal functions and external parties, including engagement with The Ethics Centre. Accountability for ethical conduct is reflected in performance management, remuneration, promotion and consequence management processes for both employees and partners.

The Firm supports reporting of ethical misconduct through various speak-up mechanisms including confidential reporting channels and whistleblower protections, with retaliation monitoring processes in place. Ethics education is delivered throughout an individual's career lifecycle including induction, continuing professional development and scenario-based learning. There is an underlying aim to move from awareness into practical action – seen through the Ethics Exchange Series pilot being run with Partners. Employee surveys, deep dive culture assessments, feedback mechanisms, ethics-related metrics and benchmarking activities are used to monitor cultural indicators and identify areas for improvement – with quarterly monitoring of progress.

While no findings were identified, several opportunities for enhancement were noted as suggestions. These include strengthening awareness of confidentiality obligations through guidance, training and practical examples; further developing ethical decision-making capabilities; clarifying governance accountability for ethics and conduct, including consideration of an independent Chief Ethics Officer; establishing clear criteria for engaging external investigators in misconduct matters; and increasing organisational learning through communication of lessons gained from ethical conduct matters and the consequential application of accountability and disciplinary frameworks.

2. Scope

As set out in the engagement letter dated 26 June 2026 the focus of the CEO Review was on the design and implementation of the Firm's:

(a) systems and processes for the storage and handling of confidential information of audit clients (confidential information), including processes for identifying, notifying and remediating any instances of unauthorised use of confidential information as required by APES 110 *Code of Ethics for Professional Accountants (including Independence Standards)* (APES 110); and

(b) systems and processes for promoting an ethical culture within the audit function, and across the organisation/firm more broadly, including whistle blower protection policies and associated practices, as required by APES 110, ASQM 1 *Quality Management for Firms that Perform Audits or Reviews of Financial Reports and Other Financial Information, or Other Assurance or Related Services Engagements* (ASQM 1) and APES 320 *Quality Management for Firms that provide Non-Assurance Services* (APES 320).

In addition, consideration was given to the Firm's risk management framework, as required by APES 325 *Risk Management for Firms* (APES 325), specifically in relation to the risks identified, assessed and managed relating to confidential information and ethical culture.

3. Review Approach

1. At the initial scoping meeting conducted on 21 July 2026, the Firm was provided with an initial document request list, a summary of which is included in Appendix A. It is confirmed the Firm provided all the documents requested or provided satisfactory explanations where not provided. The reviewer has relied on the accuracy and completeness of any information it has received from the Firm and has not independently verified those matters.
2. Based on a review of the documents provided in item 1, as well as an outline of the systems and processes as provided by the Firm dated 26 June 2026:
 - meetings were held with senior leadership and/or the various system and process owners and/or operators
 - walkthroughs of relevant systems and processes took place and/or screenshots, or other supporting documents were sighted to evidence systems and processes in place
 - additional requests for documents and meetings took place as deemed appropriate by the reviewer
3. A report was drafted with all matters of significance discussed with the Firm at the closing meeting held on 24 September 2026 and their responses included in this report, where relevant, such that the Firm has been given a reasonable opportunity to review and discuss any issues identified by the reviewer and the opportunity to provide further material relevant to those issues.

4. About the Firm

The Firm comprises a partnership structure and forms part of a global network of independent firms. The Firm is required to comply with the requirements of KPMG International regarding governance framework, quality standards and global policies including policies relating to confidential information and ethics. As a KPMG member firm it is responsible for its own obligations and liabilities.

As at 30 June 2025, the Firm had 1,655 audit client service staff and 120 audit partners operating out of all 14 Australian offices, with revenue relating to the audit of financial statements comprising 21% of the Firm's total revenue of \$2.315 billion (source: 2025 Transparency Report).

In total the Firm had 8,438 staff and 657 partners. (source: 2025 Impact Plan)

The Firm has a System of Quality Management (SoQM) supported by an iterative risk assessment process (I-RAP) designed to support compliance with APES 325, relevant systems, policies and processes that provide a structured approach to enable achievement of the objectives of ASQM 1, APES 320 and APES 325.

The Firm's National Governance Board (Board) is responsible for oversight and monitoring of the firm's management, including ensuring there are processes in place for identifying and managing risk and reputational matters. There is separation of the Board and Management.

Under KPMG's Partnership Agreement, the Board appoints a Chief Executive Officer (CEO) who is charged with responsibility for effectively managing the firm against the firm's strategy, plans and policies as approved by the Board, and the implementation of regulatory and risk management procedures across the business. The CEO leads the firm's principal management body, the National Executive Committee (NEC).

5. About the Report

The report provides an overview of the key systems and processes observed during the review, including those considered to be of a best practice nature – Parts 6 and 7, and separately in Parts 8 and 9, details of any findings and suggestions. The absence of a finding or suggestion should not be understood as confirmation that no deficiency, breach or other issue exists.

The CEO Review was conducted over systems and processes in place at the time of the review. It did not take into account future actions or planned initiatives, unless they had already commenced. However, where relevant, those already identified by the Firm are referenced in the report.

This report contains confidential and commercially sensitive information provided for the purposes of the CEO Review. This report must be handled in accordance with the confidentiality obligations set out in the Letter of Engagement between CA ANZ and your Firm and must not be disclosed except as authorised by the Letter of Engagement.

For the purposes of this report, the terms whistleblowing or whistleblower have been restricted to the actual KPMG Whistleblower Policy as published on its [website](#). Instead, reference is made to the term used by the Firm of Speak Up. In addition, terms such as raising ethical issues or concerns have been applied as set out in [IESBA's Firm Culture and Governance Dialogues booklet](#).

The CEO Review conducted by CA ANZ or the Reviewer does not form an approval, verification, opinion or acknowledgment by CA ANZ or the Reviewer that the work done or the opinions given by the Firm generally, or on particular clients, is correct or of a high or any particular standard. CA ANZ expressly disclaims all liability for any loss or damage arising from any reliance upon the fact that CA ANZ conducts the Quality Review Program or has reviewed a particular firm in the course of the Quality Review Program, or upon any annual reports, overviews, reports on particular firms, or other materials produced by CA ANZ regarding or in connection with the Quality Review Program.

The CEO Review is not a substitute for the Firm keeping itself informed as to and complying with all appropriate standards, rules, and obligations. The CEO Review provides no guarantee as to whether the conduct of the Firm is appropriate.

6. Summary of key design elements and initiatives relating to the storage and handling of confidential information of audit clients including processes for identifying, notifying and remediating any instances of unauthorised disclosure and use of confidential information.

6.1 Governance and accountability

The Firm has established a governance framework that promotes the protection of audit confidential information and reinforces the ethical obligations of partners and staff. Confidentiality requirements are embedded within the Firm's Code of Conduct, engagement terms and related policies. Clear accountability is assigned to partners and staff for safeguarding audit confidential information, supported by annual confirmations required of all partners and staff. The framework is further supported by formal escalation protocols that enable actual or suspected confidentiality incidents to be promptly brought to the attention of appropriate personnel for assessment and action.

6.2 Access and Information Security Controls

The Firm maintains a range of information security controls designed to safeguard audit confidential information throughout its lifecycle. Access to systems (including KPMG Clara, the audit technology platform), audit files and client data repositories is managed through user access controls and periodic access reviews to ensure information is available only to authorised personnel. Secure firm portals are promoted as the preferred method for exchanging information with clients and other stakeholders, supported by data classification and acceptable use requirements. Additional controls govern the use of portable storage devices, printing and electronic engagement documentation retention practices, while specific procedures are in place to ensure heightened protection of particularly KPMG Restricted client information. Ongoing monitoring of access to audit files and confidential information repositories further supports the protection of client information.

6.3 Operational initiatives

It is considered the Firm actively promotes a culture of confidentiality through a combination of mandatory training, awareness activities and guidance for personnel. Confidentiality obligations are addressed as part of induction and ongoing training programs, with periodic awareness campaigns and communications reinforcing key expectations and emerging risks. Personnel are provided with guidance on confidentiality matters commonly encountered during audit engagements, including the appropriate handling and use of client information. These initiatives are supported by a suite of technology and cybersecurity safeguards designed to help protect information from unauthorised access, use or disclosure.

6.4 Detection and Escalation

The Firm has established monitoring processes and data loss prevention capabilities designed to support the identification of actual or potential data breaches involving audit confidential information. These arrangements assist in detecting unauthorised access, use or disclosure of confidential information and ensure that potential issues are promptly brought to the attention of appropriate personnel. Documented incident identification, reporting and escalation procedures provide a clear mechanism for assessing and triaging suspected data breach incidents, including consideration of any client, regulatory or legal notification obligations that may arise.

6.5 Investigation and Remediation

Once a data breach incident involving audit confidential information has been identified and escalated, the Firm's incident response framework guides the investigation and resolution process. Investigation procedures are designed to establish the nature, scope and impact of the incident and identify any underlying causes. Where necessary, corrective and remediation actions are implemented to contain and limit any loss or damage including following notification protocols in line with contractual, regulatory or network requirements. As part of its ISO 27001 Information Security (ISO 27001) certification process, the Firm is required to perform root cause analysis to identify opportunities for enhancement to its control environment and incorporates lessons learned into its risk management practices. Follow-up activities are undertaken to assess the effectiveness of remediation measures and support the ongoing strengthening of controls around confidential information.

6.6 Monitoring and compliance

The Firm regularly assesses risks relating to the protection of confidential information, both at an enterprise level and through the risk assessment processes established under its SoQM framework. The identified risks are addressed through a range of controls, which are subject to ongoing monitoring and compliance activities, including by internal audit, which evaluate the design and operating effectiveness of information protection controls over both internal systems and client data. The results of these activities, where relevant, are considered as part of the Firm's annual evaluation of its SoQM. As part of that evaluation process, relevant leaders complete annual certifications in relation to SoQM processes and controls within their areas of responsibility. Based on that evaluation, the Firm concluded in November 2025 that, as at 30 September 2025, the SoQM provided the Firm with reasonable assurance that the objectives of the SoQM were being achieved.

The Firm's commitment to information security is further supported through its ISO 27001 certification program and associated external assessments. The most recent recertification was dated 17 February 2026. These periodic reviews of confidentiality controls and related policies contribute to management's ongoing evaluation of the effectiveness of the Firm's information security framework and its ability to respond to evolving risks.

7. Summary of key design elements and initiatives for promoting an ethical culture within the audit function, and across the organisation/Firm more broadly, including whistleblower protection policies and associated practices.

7.1 Ethical Leadership and Tone from the Top

The Firm's senior leadership demonstrates a commitment to ethical behaviour and acting in the public interest, establishing ethics as a fundamental component of the Firm's culture and professional responsibilities. Integrity is the first of KPMG's five key values, alongside Excellence, Courage, Together and For Better. Ethical considerations are embedded within the Firm's governance arrangements, strategy and operational activities, including support of initiatives in ethical leadership via the Ethics Champions network, reinforcing the expectation that ethical

values are prioritised alongside commercial and business considerations. Consistent communication from leadership reinforces the Firm's ethical values, behavioural expectations and commitment to maintaining the trust and confidence of clients, regulators and other stakeholders.

7.2 Governance and Oversight of Ethical Culture

The Firm has established governance arrangements that support the promotion, oversight and continuous reinforcement of its ethical culture. Ethical culture and conduct are regularly monitored at the Board and NEC level and evaluated through established governance processes, enabling leadership to assess the effectiveness of existing processes and initiatives and identify opportunities for enhancement. Reporting on ethics-related matters by the Chief Risk Officer to relevant leadership and governance bodies reflects the Firm's ongoing commitment to maintaining an ethical culture.

7.3 Independent Challenge and Ethical Oversight

Investigations relating to ethical conduct matters are conducted through the Firm's documented process, supported by internal functions including the dedicated Employee Relations team and the Office of General Counsel. In addition, particularly for high-risk matters, independent input is incorporated into governance and decision-making processes. This may include engagement with external advisers, independent Board members, or other suitably qualified individuals who are able to provide objective perspectives and constructive challenge independent of the Firm's management and operational functions.

KPMG's engagement with The Ethics Centre, where it has corporate membership, in its training with partners and the development of the Ethics Champion Network is also noted as a part of gaining independent and impartial perspectives.

7.4 Accountability and Ethical Responsibility

The Firm promotes a culture in which all partners and staff understand their individual responsibility for upholding its Values, professional standards and the public interest. Clear roles, responsibilities and behavioural expectations reinforce personal accountability and emphasise that ethical conduct is the responsibility of every individual, regardless of role or seniority.

Partners and staff are expected to exercise professional judgement consistent with the Firm's values, policies and ethical obligations and to take responsibility for their decisions and actions.

7.5 Ethics in Performance, Reward and Consequence Management

The Firm's performance, reward and consequence management arrangements are designed to align incentives and accountability mechanisms with its ethical values and expected standards of conduct. Values-aligned behaviour is considered alongside technical competence, leadership, quality and business performance when assessing performance across the Firm. For employees, performance evaluation, remuneration, promotion and career progression processes incorporate consideration of behaviours that align with the Firm's values, including that of integrity.

For partners, ethical conduct forms an integral component of partner performance assessment, accountability and remuneration frameworks, including considerations relating to leadership, quality, risk management and stewardship responsibilities. Recognition, promotion and reward mechanisms are designed to support behaviours consistent with the Firm's values, while consequence management processes, including clear guidelines, reinforce accountability where conduct does not meet expected standards.

Through these arrangements, the Firm reinforces the importance of integrity, professional behaviour and ethical decision-making across all levels of the organisation.

7.6 Open Discussion, Speak-Up Culture and Whistleblower Protection

The Firm seeks to foster an environment of open discussion and constructive challenge in which partners and staff are encouraged to raise concerns, seek guidance and discuss ethical matters in a respectful and psychologically safe manner. Speak-up mechanisms, common escalation pathways and confidential reporting channels (including both a local and global Whistleblower Hotline), exist to support the identification and consideration of ethical issues. The firm's Whistleblower Policy goes beyond the Corporations Act 2001 requirement to include all current partners and employees and complements the Respect@Work policies which cover workplace complaints and grievances.

Ethical concerns raised through these channels are considered through established processes, and oversight activities support the monitoring of whistleblower matters and associated outcomes. There are clear associated protections, including a Retaliation Monitoring System, designed to encourage reporting without fear of retaliation, reinforcing the Firm's commitment to openness, accountability and ethical conduct.

Collectively, these arrangements are designed to strengthen trust, encourage transparency and support the early identification and resolution of ethical issues.

7.7 Ethics Education and Awareness

The Firm invests in ongoing ethics education and awareness initiatives, such as the Ethics Champions Network, designed to develop ethical judgement, professional scepticism and confidence in addressing complex ethical matters. Ethics training is embedded within induction programs and supported through continuing professional development activities throughout an individual's career with the Firm. Training programs incorporate practical scenarios and ethical dilemmas relevant to the Firm's service lines, enabling participants to apply ethical principles to real-world situations. Firmwide mandatory learning includes specific focus on Integrity including how to Speak Up safely and confidently with specific reference to the Whistleblower Policy.

7.8 Transparency and Communication

The Firm promotes transparency through regular communication of ethical expectations, values and behavioural standards. Leadership communications cover initiatives such as outputs from culture surveys, designed to strengthen ethical culture. Reporting on ethics and conduct

activities supports accountability to leadership, governance bodies and other stakeholders, while reflecting the Firm's commitment to ethical behaviour and the public interest. These practices contribute to a culture of trust and seek to reinforce confidence in the Firm's approach to ethics and professional conduct.

7.9 Continuous Improvement and Culture Monitoring

The Firm, through its structured employee listening approach, has a continuous improvement lens in its efforts to strengthen its ethical culture. These include the annual enterprise-wide survey, annual pulse survey, employee lifecycle surveys, targeted culture surveys with specific questions on ethics and values and inclusion assessments, and ongoing employee feedback via a third-party platform.

These feedback mechanisms and other monitoring activities are used by the Culture Team within People & Inclusion to enable deep dives into specific areas of the firm as necessary, make recommendations and assess the effectiveness of ethics-related initiatives and the overall cultural environment.

Ethics-related metrics and reporting assist leadership in monitoring trends, assessing progress against desired outcomes and identifying and following up on emerging areas of focus. The Firm also benchmarks selected ethics and culture indicators against global network and industry metrics, where available, to provide context for the identification of enhancement opportunities. Where opportunities for improvement are identified, the Firm undertakes analysis of contributing factors and uses these insights to inform future initiatives which are monitored quarterly by Business Partners within the organisation. This ongoing cycle of monitoring, benchmarking, evaluation and continuous improvement supports the maintenance and ongoing development of the Firm's ethical culture and its commitment to acting in the public interest.

8. Findings

Area	Findings	Firm Response
Confidential Information of audit clients		
Governance and accountability		
Access and Information Security Controls		
Operational initiatives		
Detection and Escalation		
Investigation and Remediation		
Monitoring and Compliance		
Promotion of an ethical culture within the audit function, and the organisation more broadly		

Ethical Leadership and Tone from the Top		
Governance and Oversight of Ethical Culture		
Independent Challenge and Ethical Oversight		
Accountability and Ethical Responsibility		
Ethics in Performance, Reward and Consequence Management		
Open Discussion, Speak-Up Culture and Whistleblower Protection		
Ethics Education and Awareness		
Transparency and Communication		
Continuous Improvement and Culture Monitoring		

Any “Firm Response” recorded in the above table records the Firm’s position as communicated to the reviewer during the CEO Review. Its inclusion does not indicate that the reviewer or CA ANZ accepts, endorses or has independently verified that response, unless this report expressly states otherwise.

9. Suggestions

Any suggestions in this report are directed to the circumstances observed during the CEO Review. They do not prescribe the only means by which the Firm may address a finding or improve its systems and processes, and implementation of a suggestion does not, of itself, establish compliance with any professional, legal or regulatory requirement. The Firm remains responsible for determining and implementing appropriate action having regard to its particular circumstances and obligations.

In regard to the design and implementation of the Firm's approaches to confidential information and ethical culture, the following suggestions are made:

Area	Suggestions	Firm Response
Confidential Information of audit clients		
Governance and accountability		
Access and Information Security Controls		
Operational initiatives	1. All mandatory training should align to existing resources available online to partners and staff, or the latter updated as necessary, to ensure ready recall. This can be enabled by incorporating links to online resources into the training modules – requesting they be bookmarked.	KPMG accepts this suggestion. KPMG has refreshed its <i>Confidentiality at KPMG Policy</i> and supporting guidance and completed firmwide and targeted confidentiality training. KPMG has also required partners and staff to attest to their understanding of the updated <i>Confidentiality at KPMG Policy</i> and supporting guidance. KPMG will consider opportunities to strengthen links between relevant training modules and supporting online resources. <i>KPMG Action Plan #1.2.3, #1.3.3, #1.3.4, #1.3.6a and #1.3.6b</i>

Area	Suggestions	Firm Response
	2. Expectations regarding the appropriate use of information obtained during professional engagements to be made clear through guidance or FAQs within the firm. For example, Confidentiality policy or audit specific guidance to include clear examples of the types of audit client information considered as confidential, as aligned with the firm's Data Handling and Classification policy.	KPMG accepts this suggestion. KPMG has refreshed its <i>Confidentiality at KPMG Policy</i> and supporting guidance, including clarifying what constitutes confidential information and when information may be shared internally. KPMG has also refreshed its audit pursuit policies and procedures to strengthen ethical barriers relating to the use of audit client information in pursuit activities and completed firmwide and targeted Audit & Assurance confidentiality training. KPMG has also required partners and staff to attest to their understanding of the updated <i>Confidentiality at KPMG Policy</i> and supporting guidance. KPMG commenced a review of repositories used to store client information to assess the adequacy of existing controls and inform repository rationalisation, and control enhancement activities. Relevant workspaces have been restricted to authorised teams. KPMG will consider whether further practical examples or FAQs would assist personnel in applying these requirements. <i>KPMG Action Plan #1.2.3, #1.3.2, #1.3.4, #1.3.5 and #1.3.6a and #1.3.6b</i>

Area	Suggestions	Firm Response
	3. Training for all partners and relevant staff to emphasise restrictions on using audit confidential information for pursuits. This can be through measures such as business development activities using publicly available information or information with appropriate client consent.	KPMG accepts this suggestion. KPMG has refreshed its audit pursuit policies and procedures to strengthen ethical barriers relating to the use of audit client information in pursuit activities and completed firmwide and targeted Audit & Assurance confidentiality training. KPMG has also required partners and staff to attest to their understanding of the updated <i>Confidentiality at KPMG Policy</i> and supporting guidance. These measures reinforce the appropriate use of client information in pursuit activities. <i>KPMG Action Plan #1.3.2, #1.3.3, #1.3.4, #1.3.6a and #1.3.6b</i>
Detection and Escalation		
Investigation and Remediation		
Monitoring and Compliance		
Promotion of an ethical culture within the audit function, and the organisation more broadly		
Ethical Leadership and Tone from the Top	4. Work to further embed an ethical decision-making skillset across the firm by ensuring the existing CARE Ethical Decision Making Framework features in practical training and is applied during relevant decision-making.	KPMG accepts this suggestion. KPMG agrees with the importance of practical ethical decision-making capabilities. KPMG will consider how the CARE framework and ACCEPT principles can be further embedded through its training and broader

Area	Suggestions	Firm Response
		ethics and cultural initiatives, including the enhancement of the Ethics Champions Network. <i>KPMG Action Plan #2.5 and #2.6; Andrews Group Recommendations #1 and #5</i>
Governance and Oversight of Ethical Culture	5. Responsibility for ethics and conduct should be clearly defined within the Firm's governance structure to provide appropriate oversight of ethical matters and reinforce leadership accountability. Currently, the accountability for ethical culture is shared across firm leadership and is supported by various business services functions in how this is enabled through decision making support, reporting, learning and development, and consequences for ethical misconduct. It is recommended that an independent Chief Ethics Officer be appointed to provide oversight of the firm's ethics framework, including monitoring ethical behaviour, evaluating the effectiveness of ethics-related controls, supporting and involvement, as required, in the assessment of misconduct matters and accountability, and fostering continuous improvement in ethical culture and conduct.	KPMG accepts this suggestion. KPMG agrees with the importance of clear accountability and oversight for ethics and conduct. While the immediate focus remains on delivering the commitments set out in the remediation Action Plan, the broader objective is to embed sustainable behavioural, cultural and governance change across the firm. Success will ultimately be measured not by the completion of actions alone, but by the extent to which these changes become embedded in how we lead, make decisions and operate day to day. A complementary Implementation and Change Plan will be developed to support delivery of the remediation Action Plan and drive sustainable change across the firm. KPMG has accepted the Andrews Group recommendations to appoint a Whistleblower Protection Officer and establish an Integrity Office, with clear governance, reporting lines and independence from client-facing work, while ensuring that we meet our regulatory obligations and align with KPMG network requirements.

Area	Suggestions	Firm Response
		The Chief Ethics Officer suggestion will be considered through the design of the Integrity Office and the broader review of ethics governance arrangements including the Action Plan updates to Board Governance. <i>KPMG Action Plan #1.1.3; Andrews Group Recommendations #2 and #3</i>
	6. There is a firmwide role set out pursuant to the KPMG Australia Partnership Agreement – Ethics & Independence Partner (EIP) – however the remit for the role is specifically related to independence policies and ethical matters relevant to independence. There is also an Ethics & Independence Disciplinary Committee which only relates to disciplinary matters relating to independence policies and ethical matters relevant to Independence. It is recommended the role and committee titles be amended to more accurately reflect the narrower independence-related scope of these functions.	KPMG accepts this suggestion. The titles and remit of the Ethics & Independence Partner and the Ethics & Independence Disciplinary Committee will be considered as part of the broader review of the Firm's governance and ethics arrangements, having regard to the Partnership Agreement and applicable KPMG network requirements. <i>KPMG Action Plan #1.1.3 and #1.2.2; Andrews Group Recommendation #3</i>
Independent Challenge and Ethical Oversight	7. The Firm should consider establishing clear criteria for determining when an external independent investigator should be engaged for whistleblower or ethical misconduct matters. This could be incorporated into the existing risk-based case category framework.	KPMG accepts this suggestion. As part of the ongoing review of its whistleblower program, KPMG will consider whether additional risk-based criteria or guidance should be established for determining when an external independent investigator should be engaged.

Area	Suggestions	Firm Response
		<i>KPMG Action Plan #1.2.4 and #2.5; Andrews Group Recommendation #4</i>
Accountability and Ethical Responsibility		
Ethics in Performance, Reward and Consequence Management		
Open Discussion, Speak-Up Culture and Whistleblower Protection	8. There should be clarity (and consistency) in the language used in policies, training and communications regarding Whistleblower complaints versus grievance/workplace complaints and how they are managed. Although it is clear the differences are understood by People & Inclusion and Risk, the varying references to respectful behaviour, Respect@Work policies, integrity, ethics, ethical behaviour, ethical culture, ethical standards, grievances, misconduct, speaking up, raising concerns and whistleblowing can be confusing.	KPMG accepts this suggestion. KPMG agrees that relevant terminology and escalation pathways should be clear and consistent. KPMG will consider this as part of the ongoing review of its whistleblower policies, procedures, training and broader whistleblower program. <i>KPMG Action Plan #1.2.4 and #1.2.5; Andrews Group Recommendation #1, #3 and #4</i>
Ethics Education and Awareness		
Transparency and Communication	9. Leaders should share insights and lessons from real ethical conduct matters in communications to reinforce organisational learning and illustrate the consistent application of the firm's accountability and disciplinary framework, including appropriate consequences for misconduct. This should be in addition to any real-life scenarios used for training purposes.	KPMG accepts this suggestion. KPMG recognises the importance of organisational learning from ethical conduct matters. KPMG will consider opportunities to communicate de-identified lessons through leadership communications and training, subject

Area	Suggestions	Firm Response
		to relevant privacy, confidentiality, legal and whistleblower protection requirements. KPMG has also strengthened the governance and application of our consequences framework to further discourage misconduct, ensuring appropriate sanctions and consequences if misconduct occurs. Proposed enhancements are currently progressing through KPMG's governance and approval processes and will provide greater transparency on how and when consequences are determined and applied, including through ongoing training and governance reforms in future versions of our Action Plan. This approach reflects our intention to continue to augment, strengthen and refine remediation focus in response to external, third party and regulatory processes. <i>KPMG Action Plan #1.2.1a and #1.2.1b</i>
Continuous Improvement and Culture Monitoring		

Appendix A – Documents requested for CEO Review

Item	
1	Transparency report and/or firm annual report which includes reporting on compliance with ethical requirements.
2	ASIC inspection report and audit quality action plan.
3	Reports from any other audit external regulators (PCAOB, CPAB, etc.).
4	Internal review reports from the past 5 years with findings related to audit confidentiality and/or firm ethical culture, including associated action plans and remediation programs.
5	Local and network policies relating to confidentiality, handling and storage of client information, data breach reporting, and complaint/investigation processes.
6	Details of self-assessments undertaken in relation to compliance with network policies, including outcomes of annual risk declarations, compliance registers and breach registers.
7	Risk Management Framework entries relating to confidentiality and ethical requirements, including risk assessments and risk owners.
8	Root Cause Analysis reports, remediation plans, monitoring activities and actions relating to confidentiality or ethical requirements.
9	Staff and partner performance evaluation framework documentation setting out performance criteria.
10	Consequence management framework for partners and staff, including outcomes and communication processes.
11	Audit and/or firmwide training relating to confidentiality and ethical culture, including reporting of allegations or complaints.
12	Evidence of how ethical culture is communicated and reinforced by leadership, including newsletters, quality bulletins, surveys and whistleblower channels.
13	Organisation charts for audit and compliance functions relating to confidentiality, including detection and prevention activities.
14	Standard engagement terms for audit engagements or other documents setting out confidentiality provisions.
15	Details of reporting to clients, regulatory authorities or professional bodies relating to breaches of confidentiality.
16	Organisation charts for audit and whistleblower protection functions, including escalation pathways and leadership involvement.
17	Details of skills, experience and prerequisites required for personnel involved in investigating formal and informal complaints.
18	Details of audit quality objectives relating to ethical requirements, assessed risks, responses and alignment with the firm risk management framework.
19	Details of systems and resources used to support reporting of whistleblower complaints and allegations.

Note: Appendix A contains a summarised version of the initial document request list provided to the Firm. It does not reproduce the full request list and does not include additional documents subsequently requested or otherwise reviewed during the CEO Review.

Appendix B – List of interviewees

Meeting	Role
Audit and Assurance, including Internal Audit	SoQM Country Leader / Divisional Risk Management Partner – Audit & Assurance Partner, Consulting (Internal Audit) Director, Consulting (Internal Audit) Director, Audit & Assurance (Internal Protection Controls Review)
Technology	Chief Digital Officer ¹ Risk Management Partner - Digital Risk & Security Governance
Ethics and Independence	Ethics and Independence Partner
People & Inclusion	National Managing Partner, People & Inclusion ¹ Partner, People & Inclusion Director, Employment Risk Associate Director, Culture and Inclusion Lead
Quality and Risk	Chief Risk Officer ¹ Privacy Officer Director – Risk Management

¹ Member of the National Executive Committee