



Introduction

This quarterly publication provides a comprehensive summary of key developments in financial reporting, sustainability, governance and regulation, together with practical insights into the emerging risks shaping corporate decision-making.

The June quarter has reinforced a common theme across regulators and standard setters: accountability. Whether in financial reporting, sustainability disclosures, cyber resilience or risk governance, organisations are being challenged to demonstrate that processes, controls and judgements are capable of withstanding increased scrutiny.

With the 30 June reporting season underway, ASIC has highlighted valuation practices, reporting quality and governance responsibilities as priority areas, while early observations on mandatory sustainability reporting are beginning to shape expectations for future reporting periods. At the same time, regulators continue to warn that emerging technologies, cyber threats and geopolitical uncertainty are creating new and interconnected risks that require greater board oversight and organisational preparedness.

This edition explores these developments and their implications for directors, audit committees, finance leaders and risk professionals operating in a rapidly evolving regulatory environment.



Highlights

Financial reporting

- ASIC's 30 June focus areas
- ASIC hones in on non-lodgements
- Bulky Tier 3 standard arrives
- Private credit on notice over valuations

Sustainability reporting

- ASIC's early observations on sustainability reporting
- ASIC updates sustainability FAQs

Governance

- Directors fined for DIN non-compliance
- APRA warns on AI-related risks
- Five eyes on AI and cyber security

Regulators

- Get ready for geopolitical shocks, says APRA
- Pay-day super begins on 1 July
- New national minimum wage

ASX

- First ASX supervision report released

AFSLs

- ASIC calls for boost in cyber resilience

Ethics

- IESBA releases Q&As on using technology

Financial reporting

ASIC's 30 June focus areas

In keeping with ASIC's enduring financial-reporting focus areas (see appendix), the commission will monitor financial-report preparers' major judgements. They are predominantly in revenue recognition, assessment of asset impairment, and recognition and measurement of financial instruments.

Refreshing 30 June valuations is a must-do, especially for private credit and across private investments generally. If valuations fail to reflect current conditions and incorporate verified accurate information the risk of misinformation and poor investor outcomes is higher.

ASIC expects professionals to challenge assumptions and refresh valuations to ensure that they are based on realistic and supportable inputs. They should ensure that financial reporting, audit, and assurance practices support 30 June valuations. Market participants should not wait for formal defaults before reassessing asset values and related risks.

In 2026-27, ASIC will review the financial reports of listed and unlisted companies, registrable superannuation entities, and managed investment schemes.

The commission will also review disclosures of companies that make provisions for decommissioning and site restoration costs. The reviews will assess disclosures against new guidance issued by the AASB (illustrative example D of AASB 137 *Provisions, Contingent Liabilities and Contingent Assets*).

The commission reminds us that directors and superannuation trustees are primarily responsible for the quality of financial reports in accordance with the *Corporations Act 2001* and applicable Australian accounting standards. This includes ensuring that management produces high-quality and timely financial information supported by robust position papers with appropriate analysis and conclusions.

Appropriate experience and expertise should be applied in the reporting process, particularly in more difficult and complex areas, such as asset valuations, provisions, revenue arising from contracts with customers, capitalisation of expenditure, expected credit losses and other estimates, the impact of post-balance-date events, and disclosure.

The basis and circumstances related to management's judgements on accounting estimates and forward-looking information should be documented at the time and disclosed in financial reports.

ASIC hones in on non-lodgements

Financial reporting misconduct, including the failure to lodge financial reports, is one of ASIC's 2026 enforcement priorities.

The commission has issued infringement notices with financial penalties of \$198,000 to three companies operating major fashion and beauty retail businesses for allegedly failing to lodge financial reports by required dates.

ASIC commissioner Kate O'Rourke said that the infringement notices reinforced (the commission's) commitment to acting on late and non-lodgement of financial reports by large proprietary companies.

'Since announcing a broad surveillance focused on late lodgement and non-lodgement of financial reports in August 2025, ASIC has issued 24 infringement notices totalling over \$4.5 million for alleged financial-reporting breaches.

'This, combined with court-imposed fines for failing to lodge financial reports and related governance obligations, should send a clear message to reporting entities that we are actively enforcing the financial reporting requirements and expect companies to comply.

'In line with our current enforcement priority, and through our targeted, data-driven surveillance, we continue to identify and investigate a number of companies that have lodged late or failed to lodge at all.

'ASIC will take appropriate action to ensure reporting entities are well aware of, and comply with, this important governance and disclosure obligation.'

As well as issuing 24 infringement notices, the commission has obtained court-imposed penalties, including more than \$1.1 million in fines, of three public companies.

Large proprietary companies are obliged to prepare and lodge annual financial reports. A proprietary company is classified as 'large' if it meets at least two of the following criteria for a financial year:

- Consolidated revenue of the company and any entities it controls is \$50 million or more
- Consolidated gross assets of the company and any entities it controls is \$25 million or more, and
- The company and any entities it controls have 100 or more employees.

These criteria are to be determined by the application of accounting standards issued by the AASB. Such a determination can be challenging.

Other entities obliged to lodge financial reports include public companies, registered managed investment schemes, registrable superannuation entities, and small proprietary companies that are controlled by a foreign company.

Financial reporting

Bulky Tier 3 standard arrives

AASB 1061 *General Purpose Financial Statements – Not-for-Profit Private Sector Tier 3 Entities* focuses on information that ‘matters most to users of smaller NFP financial statements, cutting unnecessary complexity’.

The result is a better proportioned general-purpose reporting option that helps smaller NFPs prepare financial statements more efficiently, freeing up time and resources to stay focused on mission and service delivery.

The package also includes AASB 2026-2, which amends Australian standards to extend the application of the Conceptual Framework and limit the ability of NFP entities to prepare special-purpose financial statements. It contains amendments to more than 30 standards and interpretations.

The new standards will be effective for annual reporting periods beginning on or after 1 July 2029, early application permitted.

The Australian Accounting Standards Board will continue working with regulators, legislative bodies, and relevant government agencies to support consistent and effective implementation across the NFP sector.

Private credit on notice over valuations

The private credit sector is facing its first real test. Tighter liquidity, emerging borrower stress, and signs of credit deterioration are testing valuations, governance, and investor disclosures.

ASIC is calling on funds to ensure that their 30 June asset valuations are current, accurate, and grounded in realistic assumptions.

ASIC expects boards, auditors, and participants across the private-credit eco-system, including responsible entities, trustees, and chief investment officers, to assess private credit and broader private market practices against the commission’s 10 principles and lift standards where needed.

Poor practices in private credit remain a 2026 enforcement priority, and ASIC has said that it will act where conduct falls short.

Obligations cannot be outsourced. Participants must ensure that those involved in their funds – management value chains from origination through to audit – are meeting their responsibilities to support participants’ obligations.



Financial reporting

ASIC's message is straightforward: participants should use this reporting cycle to challenge assumptions, refresh valuations, and lift practices in line with the 10 principles.

Principle	Explanation
Stewards of other people's money	Responsible entities and trustees act as stewards of investor capital, ensuring that their decisions are fair and in investors' best interests
Organisational capability	Human, financial and technological resources are adequate. Responsible entities and trustees operate efficiently, honestly and fairly
Transparency	Investors have access to timely, transparent information on investment strategy, exposures, valuations, risks, and fees
Design and distribution	Practices are fair, transparent, and appropriately targeted for investors
Fees and costs	Fair and transparent, giving investors and borrowers a clear view of total costs
Conflicts of interest	Identified, disclosed, and effectively managed or avoided
Governance structures	Processes and people promote sound decision-making, compliance, and accountability
Valuations	Are fair, timely, and transparent, with robust governance
Liquidity	Liquidity risk is effectively disclosed and managed, avoiding structural mismatches, with fair redemption terms aligned to portfolio liquidity
Credit risk	Credit risk is effectively managed across loan origination, portfolio construction, monitoring, impairment, default, and repayment

Private credit and private markets generally should refresh 30 June valuations. If they fail to reflect current conditions and incorporate verified accurate information there is a higher risk of misinformation and poor investor outcomes.

ASIC expects preparers to challenge assumptions to ensure that valuations are based on realistic and supportable inputs. Participants should ensure that financial reporting and audit and assurance practices support valuations. Market participants should not wait for formal defaults before reassessing asset values and related risks.



Sustainability reporting

ASIC's early observations on sustainability reporting

ASIC has published observations on initial sustainability reports prepared under Chapter 2M of the *Corporations Act 2001* to assist entities ahead of 30 June.

The review considered whether the reports provided high-quality information useful for decision-making that complies with the act and AASB S2 *Climate-related Disclosures*.

It found a marked improvement in both the quantity and quality of climate-related financial information, particularly compared with earlier voluntary disclosures. The introduction of standardised requirements also appeared to promote consistency and improve information clarity. ASIC noted that tables and diagrams presented information well.

The review also identified opportunities for entities to enhance their sustainability reporting. The commission encouraged them to consider the following when preparing reports:

- Do not include disclaimers that conflict with the statutory framework and objectives of Chapter 2M, as these can mislead or confuse
- Use all reasonable and supportable information – covering past events, current conditions, and forecast future conditions – when identifying climate-related risks
- Disclose relevant judgments, assumptions, and measurement uncertainties clearly and effectively, ensuring that they are presented close to related information
- Avoid obscuring material climate-related financial information with additional disclosures
- When cross-referencing information outside the sustainability report, entities must ensure that they meet relevant requirements, and
- Remember that 'climate-related targets' under AASB S2 include legally-required targets, such as those set by the safeguard mechanism for greenhouse-gas emissions.

Final observations will be published in the second half of 2026.

ASIC has updated its *Sustainability reporting and audit relief* decisions register to include its decisions on individual relief applications. They number 13.

ASIC updates sustainability FAQs

ASIC has updated 20 FAQs: *Review or audit of sustainability reports*. They contain guidance about the review and audit requirements of sustainability reports under the *Corporations Act 2001*.

They might help:

- Preparers understand their obligations about obtaining a review or audit of a report, the appointment/removal/resignation of auditors, and who can conduct a review or audit, and
- Auditors to understand their obligations under the act, such as stating an opinion on a report, what the auditor's report must contain, the extent to which modified liability settings apply to statements in an auditor's reporting on a sustainability report, and auditor independence.

A noteworthy FAQ is the 20th: 'What is ASIC's approach to supervision and enforcement?'

ASIC says: 'We will take a pragmatic and proportionate approach to supervision and enforcement as the review and audit requirements for sustainability reports under the Corporations Act are being phased in.'

'We are more likely to commence an enforcement investigation where we see misconduct of a serious or reckless nature.'



Governance

Directors fined for DIN non-compliance

Two New South Wales directors have been convicted and fined \$10,000 each for failing to comply with director identification obligations.

Failing to have a director identification number is a strict liability offence, meaning liability arises regardless of intent. The \$10,000 fines reflect the seriousness of the offence and serve as a deterrent.

ASIC has prosecuted 11 directors for failing to comply with DIN requirements, resulting in more than \$40,000 in fines. Obtaining a DIN is a mandatory legal requirement.

APRA warns on AI-related risks

The Australian Prudential Regulation Authority has called for a 'step-change' in how banks, insurers and superannuation trustees manage AI-related risks as the technology continues to evolve.

In a letter to industry, APRA warned that governance, risk management, assurance, and operational resilience practices are failing to keep pace with the scale, speed, and complexity of AI adoption.

The letter outlines the findings of a targeted supervisory review APRA undertook late last year across its regulated industries. The review noted that the expanded use of advanced AI is introducing a range of new financial and operational vulnerabilities, but that information-security practices are struggling to keep up with the pace of change.

The authority warned that frontier AI models such as Anthropic's Claude Mythos, which could enhance the discovery of vulnerabilities by bad actors, are expected to further increase the probability, speed, and scale of cyber-attacks.

Other key observations included:

- AI use is accelerating across all APRA-regulated industries, entities moving from experimentation towards more operationally embedded and customer-facing applications. However, governance arrangements have not matured at the same pace
- Boards have strong interest in AI's potential benefits but many lack the technical literacy to provide effective challenge to management on AI related risks and oversight
- Heightened concentration risk was noted, some entities heavily dependent on a single provider for several AI uses
- AI functionality is often embedded within broader software platforms and developer tooling, reducing transparency over where and how models are trained, updated, and constrained, and limiting entities' ability to completely assess and manage risks, and
- AI risks can cut across many domains, such as operational resilience, cyber and information security, privacy, and procurement. Existing change and assurance management approaches are often fragmented and might not effectively provide sufficient assurance.

APRA member Therese McCarthy Hockey said: 'What we've observed from our supervisory engagement is that while AI adoption is continuing apace, the systems and processes required to safely govern its use aren't keeping up. Likewise, the speed at which entities can identify, and patch vulnerabilities needs to operate much faster, commensurate with the AI-accelerated threat.

'The findings outlined in today's letter emphasise our expectations for how entities should be managing these risks in alignment with our prudential standards in areas such as information security, operational risk management, governance, and data risk.

'[We] expect to see a significant improvement in how entities are closing the gaps between the power of the technology they are using and their ability to monitor and control it.



Governance

Five eyes on AI and cyber security

AI is here. It lowers barriers for malicious actors, accelerates attacks, and narrows the window between vulnerability and exploitation. It also offers powerful tools to strengthen defence.

The Five Eyes cyber-security agencies here and in New Zealand, Canada, the UK and US urge leaders to:

- Understand and assess risk, readiness, and accountability
- Prioritise foundational cyber-security practices and controls
- Empower cyber leaders with authority and resources, and
- Stay actively engaged as threats and guidance evolve.

Success depends on getting the basics right, acting quickly, and making cyber security part of core business strategies. Those who delay face growing operational and strategic disadvantage.

Five Eyes has identified five actions. They are not new, but are urgent to reduce not only technical risk, but also operational, financial, and reputational exposure:

- Reduce your attack surface: Limit unnecessary system access and external connectivity. Challenge whether systems need to be exposed at all and isolate those that do not
- Accelerate patching processes: AI is shortening the time between vulnerability discovery and exploitation. Delays in patching increase risk, especially for operational systems with long update cycles. Prioritise security updates accordingly to manage risks
- Address legacy systems: Unsupported systems are easy targets. They are not just technical debt, they are strategic liabilities
- Review and strengthen identity and access controls: Limit who can access critical systems. Enforce strong authentication and regularly review permissions, and
- Prepare for incidents before they happen: Test response plans, train and prepare teams, and assume breaches will occur. Focus on fast containment and recovery.



Regulators

Get ready for geopolitical shocks, says APRA

The Australian Prudential Regulation Authority has written to banks, insurers and superannuation funds setting out its minimum expectations about their readiness for geopolitical shocks.

APRA has grown increasingly concerned in recent years about the potential for adverse impacts on the financial system from geopolitical shocks such as trade restrictions, sanctions, and armed conflicts.

Although most entities are aware of geopolitical risks, APRA and other agencies on the Council of Financial Regulators have observed common gaps in how entities confront them with practical risk management and crisis preparedness.

The gaps include:

- Actions by nation states to impose sanctions, restrict market access or reduce capital mobility are often not considered explicitly in business plans and credit, funding, and investment strategies
- Risk management is not keeping pace with rapidly evolving threats. These include personnel-related security risks and risks associated with disinformation campaigns that could undermine confidence in an entity's resilience
- Many boards are still developing the technical literacy needed to provide effective challenges to technology-related risks such as AI. Reliance on critical third parties, often overseas, makes it more challenging to manage risks, and

- Crisis preparedness exercises are not always strong enough to give boards and management confidence that the entity can withstand and respond effectively to a severe geopolitical shock.

APRA has written to its regulated industries setting out minimum expectations for geopolitical risk readiness in six key areas. These include enhancing preparation for non-financial and non-traditional risks such as foreign interference, insider threats, and cyber-attacks.

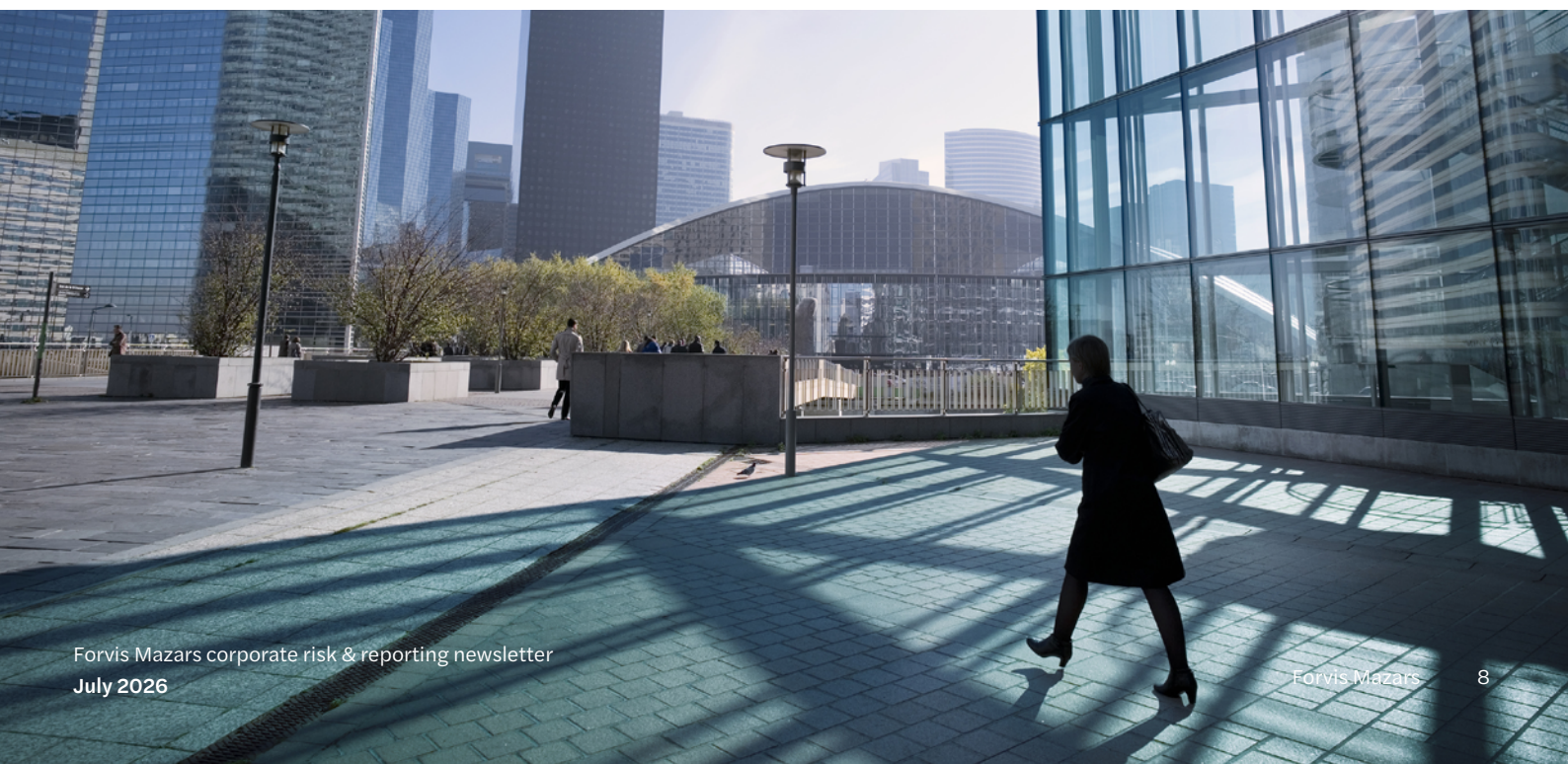
They also include an entity's preparation for traditional financial impacts through capital and liquidity planning as well as investment stress-testing for potential scenarios such as market closure, sanctions, and funding stresses.

APRA chair John Lonsdale said: 'Today's letter is a clear call to action as awareness is not enough. We need to see APRA-regulated entities integrate geopolitical risk into governance, risk management, and crisis-preparedness practices to strengthen their readiness for geopolitical shocks.'

'Where APRA identifies heightened exposure, weak governance, or inadequate preparedness, we will take appropriate supervisory action to address these gaps.'

'The expectations outlined in today's letter do not represent new prudential requirements. Rather, APRA seeks to ensure entities [to] use APRA's existing prudential standards to better integrate geopolitical risk into governance, risk management, and crisis preparedness.'

APRA will shortly write to a group of larger entities with heightened exposure to geopolitical shocks, asking them to complete a readiness assessment focusing on crisis preparedness, personnel, and political risks.



Regulators

Pay-day super begins on 1 July

From 1 July, employers will be required to deposit employees' super into accounts within seven business days of payday. The Australian Taxation Office estimates that \$6.25 billion worth of super went unpaid in the most recent financial year.

The new law will:

- Require employers to ensure super contributions are received by the employee's fund within seven business days of payday or they will be liable for the superannuation-guarantee charge
- Help the Australian Taxation Office enforce the law and more quickly identify employers not making contributions, and
- Redesign the superannuation-guarantee charge to be fit for purpose and make Payday Super work.

The ATO will monitor compliance for 12 months after the change. Its approach will differentiate between low and high-risk employers.

Employers that are trying to pay contributions in line with pay cycles can fall into a low-risk category.

The federal government has published regulations supporting the implementation of Payday Super reforms.

The *Treasury Laws Amendment Payday Superannuation Regulations 2026* confirm the kinds of payments that do not attract super and the consequences of an employer voluntarily disclosing any missed payments.

They provide a reduced three day timeframe for superannuation funds to approve or reject contributions. This aims to ensure that contributions are allocated to a member correctly and earlier, including the resolution of errors.

The taxation office's first year transitional approach *Practical Compliance Guideline 2026/1* has been published. In 2026–27, employers will not be penalised if they are doing what they can to obey the new regulations as system and software upgrades are rolled out.

New national minimum wage

The national minimum wage applies to employees who aren't covered by an award or enterprise agreement.

From 1 July, it will be: \$1004.90 per week, or \$26.44 per hour. The new amounts will apply from the first full pay period on or after 1 July.



First ASX supervision report released

ASX Supervision has released its first *Listed Entity Supervision* Report, its aim to provide an overview of the exchange's supervision and enforcement in FY26. It also provides an insight into the exchange's likely focus areas in FY27.

The report also includes updates to several topical rules matters including:

- Earnings surprises
- Committee composition
- Investor presentations
- Continuous disclosure and ramping, and
- Focus areas for disclosure by mining entities.

The ASX has made 20 referrals to ASIC. Corporations act issues covered can include a range of issues such as suspected insider trading, continuous-disclosure contraventions, misleading and deceptive conduct, directors' duties contraventions, and false and misleading statements to a market operator.

Listed entities and their advisers are encouraged to read the report.



ASIC calls for boost in cyber resilience

In an open letter to industry, ASIC is calling on licensees and market participants to urgently strengthen their cyber-resilience measures, as AI models such as Anthropic's Claude Mythos intensify cyber risks.

ASIC directs entities to table the letter at their next board and risk-governance committee meetings.

While cyber-risk has always existed, misuse of emerging AI models could expose cyber-security vulnerabilities at an unprecedented speed, scale, and sophistication, it says.

The commission has urged entities to act now and not wait for advanced AI tools to improve cyber security to withstand AI-accelerated threats.

ASIC commissioner Simone Constant emphasised the need for urgent, focused action using a principles-based, 'model-agnostic' approach, reminding industry that cyber resilience must be treated as a core licensing obligation, not simply an IT issue.

Commissioner Constant said: 'Cyber risk has entered a new era. The advent of frontier AI models creates opportunity, but also materially increases risk, with the ability to expose vulnerabilities far faster than many realise.

'Entities need to have robust incident-response plans. Whether an entity faces a basic phishing attempt or a more sophisticated cyber-attack, the underlying cyber-risk management principles of govern, protect, detect, respond remain the same.

'Appropriate cyber-risk management starts at the leadership of licensees and participants. Boards and executives must ensure systems are tested, weaknesses are addressed early, and that action is taken before threats can be exploited.'

ASIC is urging entities to take the following steps:

- Reassess your cyber plans and refocus efforts on the most critical risks in today's threat environment.
- Confirm your cyber risk, governance, and overall risk and decision-making frameworks. Consider the cumulative impact of interrelated vulnerabilities and facilitate clear decision-making and escalation at the pace necessary to manage risk.
- Identify and protect critical assets and systems, with a clear understanding of what matters most to your business and customers.
- Strengthen cyber security by regularly reviewing and validating core controls.
- Minimise attack surfaces by reducing exposure of systems and services to untrusted networks.

- Regularly review user access and reassess privileges to protect against unauthorised access. Insider threats are increasing and entities should monitor for warning signs and act to restrict access where concerns are identified.
- Patch systems promptly, recognising that AI is accelerating discovery and exploitation
- Review and strengthen patch-management processes, considering challenges daily patching may present to identification, testing, and governance of critical updates.
- Implement layered, defence-in-depth architectures that assume breach and restrict lateral movement
- Prepare for incident response by maintaining and exercising incident-response plans and playbooks, including business-continuity plans and identification of highest-priority services, channels, and platforms.
- Actively manage third-party risks, particularly where services introduce concentration or systemic exposure, and
- Use AI for defensive purposes, where appropriate, including identifying vulnerabilities and securing software before release.

ASIC encourages entities it regulates to use practical guidance from trusted sources, including the Australian Signals Directorate, to strengthen cyber defences.

Ethics

IESBA releases Q&As on using technology

The International Ethics Standards Board for Accountants has issued *Snapshots Ethics and Independence Approach to the Use of Technology* to provide short, non-technical overviews of IESBA projects and initiatives through seven Q&As.

The snapshot is relevant here as APES 110 *Code of Ethics for Professional Accountants (including Independence Standards)* is based on the International Code of Ethics for Professional Accountants issued by IESBA.

The response to Q4 'What were the 2023 technology-related revisions to the Code?' is particularly noteworthy in the context of AI use by preparers and auditors. The key changes affected were:

Area	Affect
Professional competence and due care	Understand, be able to explain, and evaluate the technology you use, including keeping pace with technology-related developments relevant to your professional activities. Relying on opaque or unexplained outputs is not acceptable.
Inquiring Mind	A prerequisite to understanding the source and relevance of inputs, and the sufficiency of technology outputs for the intended purpose. It applies to all professional accountants regardless of the activity undertaken.
Use of technology outputs	Applies whenever a professional accountant uses technology outputs whether internally developed, purchased, or third-party. Accountants must assess fitness for purpose, understand limitations and assumptions, evaluate data quality and potential bias, and determine the appropriate extent of reliance.
Automation bias	Automation bias is the tendency to favour outputs generated by technology even when contradictory information raises questions about their reliability. It is now explicitly named in the code as a bias that can impair objectivity and the proper exercise of professional judgment. The code requires accountants to be alert to this and other biases, and professional responsibility cannot be delegated to a machine.
Complex circumstances	The code includes guidance on managing complexity – defined as arising from the compounding effect of interactions among uncertain elements and interdependent variables and assumptions. Rapid digitalisation has made such circumstances more prevalent, and professional accountants must communicate inherent uncertainties to their organisation, firm, and users of their professional activities and remain alert to changes in facts and circumstances.
Confidentiality	Confidentiality obligations have been extended to cover the full data lifecycle: collection, use, transfer, storage, dissemination, and lawful destruction. The use of client data for purposes such as AI training requires proper authorisation, with clear boundaries around consent.
Independence	The independence standards have been reinforced to address risks specific to technology-enabled services: self-review threats, the risk of assuming management responsibility, and commercial dependencies that can arise when technology is used to deliver professional services to audit and assurance clients.

Appendix: ASIC's 'enduring' focus areas for financial reporting

Area	Consideration
Revenue	Directors, RSE trustees and auditors should review an entity's revenue recognition policies to ensure that: - Revenue and deferred revenue are recognised in accordance with the substance of the underlying transactions and the satisfaction of performance obligations - Judgements and assumptions used in revenue models are appropriate and reasonable, and - Disclosure of revenue policies is not boilerplate and is appropriate for each material revenue stream.
Impairment of non-financial assets	Goodwill, indefinite useful life intangible assets, and intangible assets not yet available for use must be tested annually for impairment. Entities adversely impacted in the current environment may have new or continuing indicators of impairment that require testing for other non-financial assets. The appropriateness of key assumptions supporting the recoverable amount of non-financial assets. The valuation method used for impairment testing should be appropriate, use reasonable and supportable assumptions, and be cross-checked for reliability using other relevant methods. An entity's market capitalisation will generally not represent an appropriate fair-value estimate for its underlying business but may be useful as an impairment indicator or in a valuation cross-check. Share prices may reflect transactions of relatively small proportionate interests as part of an investor's strategy for a share portfolio. Businesses may be sold in illiquid markets with few potential participants. A business acquirer may seek synergistic benefits or make significant changes to a business. Values from applying the ratio of market capitalisation to revenue for other entities to the entity's own revenue will generally be more appropriately used in valuation cross-checks. Information may be dated and the limitations in using an entity's own market capitalisation may apply. Other entities must have closely comparable businesses, products, markets, cost structures, funding, and so on. Disclosure of estimation uncertainties, changing key assumptions, and sensitivity analysis or information on probability-weighted scenarios.
Values of property	Factors that could adversely affect commercial and retail property values should be considered, such as changes in office-space requirements of tenants, on-line shopping trends, future economic or industry impacts on tenants, and the financial condition of tenants. The lease-accounting requirements and the impairment of lessee right-of-use assets.

Appendix: ASIC's 'enduring' focus areas for financial reporting

Area	Consideration
Expected credit losses on loans and receivables	Whether key assumptions used in determining expected credit losses are reasonable and supportable. Any need for more reliable and up-to-date information about the circumstances of borrowers and debtors. Short-term liquidity issues, financial condition and earning capacity of borrowers and debtors. Ensuring the accuracy of ageing of receivables. Using forward-looking assumptions and not assuming recent debts will all be collectible. The extent to which history of credit losses remains relevant in assessing ECLs. Whether possible future losses have been adequately factored in, using probability-weighted scenarios, as necessary. Disclosure of estimation uncertainties and key assumptions. ECLs should be a focus for companies in the financial sector. Financial institutions should have regard to the impact of current economic and market conditions and uncertainties on ECLs. This includes assessing whether there are significant increases in credit risk for particular groups of lenders, the adequacy of data, modelling, controls, and governance in determining ECLs, and disclosing uncertainties and assumptions.
Financial-asset classification	Financial assets are appropriately measured at amortised cost, fair value through other comprehensive income or fair value through profit and loss. Criteria for using amortised cost include whether both: - Assets are held in a business model whose objective is to hold the assets to collect contractual cash flows, and - Contractual terms give rise on specific dates to cash flows that are solely payments of principal and interest on the principal outstanding.
Value of other assets	The net realisable value of inventories, including whether all estimated costs of completion and necessary to make the sale have been considered in determining net realisable value. Whether it is probable that deferred tax assets will be realised. The value of investments in unlisted entities.
Provisions	The need for and adequacy of provisions for matters such as onerous contracts, leased property make-good, mine-site restoration, financial guarantees given and restructuring.
Subsequent events	Events should be reviewed as to whether they affect assets, liabilities, income, or expenses at year-end or relate to new conditions requiring disclosure.

Appendix: ASIC's 'enduring' focus areas for financial reporting

Area	Consideration
Disclosure – general considerations	Directors and preparers should put themselves in the shoes of investors and consider what information investors would want to know. Disclosures should be specific to the circumstances of the entity and its businesses, assets, financial position, and performance. Changes from the previous period should be considered and disclosed.
Disclosures in the financial report	Uncertainties may lead to a wider range of valid judgements on asset values and estimates. The financial report should disclose uncertainties, changing key assumptions and sensitivities. This will assist investors in understanding the approach taken, understanding potential future impacts and making comparisons among entities. Entities should also explain where uncertainties have changed since the previous full-year and half-year financial reports. The appropriate classification of assets and liabilities between current and non-current categories on the statement of financial position should be considered. This may have regard to matters such as maturity dates, payment terms, and compliance with debt covenants.
OFR disclosures	These should complement the financial report and tell the story of how the entity's businesses, results, and prospects are affected by economic and market conditions, and changing circumstances. The overall picture should be clear, understandable, and be supported by information that will enable investors to understand the significant factors affecting the entity, its businesses, and the value of its assets. The OFR should explain the underlying drivers of the results and financial position, as well as risks, management strategies, and prospects. All significant factors should be included and given appropriate prominence. The most significant business risks at whole-of-entity level that could affect the achievement of the disclosed financial performance or outcomes should be provided, including a discussion of environmental, social, and governance risks. The risks will vary depending upon the nature and businesses of the entity and its strategies. An exhaustive list of generic risks that might potentially affect a large number of entities would not be helpful. Risks should be described in context – for example, why the risk is important or significant and its potential impact and, where relevant, mitigation factors within the control of management. Climate-change risk could have a material impact on the prospects of entities and needs to be disclosed. Cyber-security risks could have a material impact for many entities and require disclosure.
Non-IFRS financial information	Any non-IFRS profit measures (i.e. measures not in accordance with all relevant accounting standards) in the OFR or market announcements should not be presented in a potentially misleading manner (see regulatory guide 230 Disclosing non-IFRS financial information).
Disclosure in half-year reports	Disclosure will also be important for half-year financial reports and directors' reports. Half-year reports should disclose information on significant developments and changes in circumstances since the last full-year report.

Appendix: Acronyms and Abbreviations

Principle	Explanation
AASB	Australian Accounting Standards Board
AFSL	Australian Financial Services Licence
AI	Artificial Intelligence
AML/CTF	Anti-Money Laundering and Counter-Terrorism Financing
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
ATO	Australian Taxation Office
DIN	Director Identification Number
ECL	Expected Credit Loss
IESBA	International Ethics Standards Board for Accountants
IFRS	International Financial Reporting Standards
NFP	Not-for-Profit
OFR	Operating and Financial Review
RSE	Registrable Superannuation Entity

Contacts

Sydney



Rose Megale
Partner, Sydney
rose.megale@forvismazars.com



James Martin
Partner, Sydney
james.martin@forvismazars.com



Mustafa Kothari
Partner, Sydney
mustafa.kothari@forvismazars.com

Melbourne



Craig Silvester
Partner, Melbourne
craig.silvester@forvismazars.com



Alexis Aupied
Partner, Melbourne
alexis.aupied@forvismazars.com



Graeme Hedding
Partner, Melbourne
graeme.hedding@forvismazars.com

Sydney

Level 12, 90 Arthur Street
North Sydney NSW 2060
Tel: +61 2 9922 1166

Melbourne

Level 5, 600 Bourke Street
Melbourne Vic 3000
Tel: +61 3 9252 0800

All rights reserved. This publication in whole or in part may not be reproduced, distributed or used in any manner whatsoever without the express prior and written consent of Forvis Mazars, except for the use of brief quotations in the press, in social media or in another communication tool, as long as Forvis Mazars and the source of the publication are duly mentioned. In all cases, Forvis Mazars' intellectual property rights are protected and Forvis Mazars Global shall not be liable for any use of this publication by third parties, either with or without Forvis Mazars' prior authorisation. Also please note that this publication is intended to provide a general summary and should not be relied upon as a substitute for personal advice. Content is accurate as at the date published.

Forvis Mazars Group SC is an independent member of Forvis Mazars Global, a leading professional services network. Operating as an internationally integrated partnership in over 100 countries and territories, Forvis Mazars Group specialises in audit, tax and advisory services. The partnership draws on the expertise and cultural understanding of over 40,000 professionals across the globe to assist clients of all sizes at every stage in their development.

Published: July 2026

forvismazars.com/au

**forvis
mazars**