RiskWise

AUDIT · RISK · ASSURANCE

Audit, risk and assurance for boards, auditors and risk professionals

EDITION 1 · DECEMBER 2026



IN THIS EDITION

The Three Lines Model, explained

Who owns risk, who oversees it and who gives assurance

The Global Internal Audit Standards

Five domains, 15 principles and what changed

A risk register that works

ISO 31000 in practice, and the limits of the heat map

Operational resilience and CPS 230

Critical operations, tolerances and service providers

Fraud, climate reporting and cyber

What the data shows and what boards must do now

Edited by Sukh Sandhu | riskwisemag.com

EDITION 1 | DECEMBER 2026

Contents

Confidence, earned 3

The Three Lines Model Explained: Who Owns Risk, Who Checks It, and Who Tells the Board 5

The Global Internal Audit Standards: What Changed, What Is Now Mandatory, and What Boards Should Ask 13

Building a Risk Register That Works: From ISO 31000 to the Boardroom 23

Operational Resilience and CPS 230: What APRA Requires, and What Every Organisation Can Learn 32

Fraud, What the Data Shows: Lessons From 2,402 Cases and the Australian Standard 42

Climate Reporting and Assurance in Australia: What the Law Requires and What Comes Next 51

Cyber Risk for Boards: The Australian Picture at November 2026 59

About RiskWise 67

EDITORIAL

Confidence, earned

By Sukh Sandhu, Editor-in-Chief

Assurance is the discipline of earning confidence rather than assuming it. RiskWise is a monthly magazine for the people who do that work, and for the boards that rely on it.

Welcome to the first edition of RiskWise. Every organisation runs on statements of confidence: that the numbers are right, that the controls work, that the supplier will deliver, that the systems will hold. Audit, risk management and assurance exist to test those statements, and the expectations on all three have risen sharply in recent years.

Internal auditors now work to new global standards. Regulated entities must show they can keep critical operations running through disruption. Large companies are reporting on climate risk, with assurance phasing in. Cyber incidents and fraud continue to cost organisations and the people they serve. Boards are expected to understand all of it well enough to ask the right questions.

In this edition

Part 1, Assurance foundations, explains the Three Lines Model and who is responsible for what, then walks through the Global Internal Audit Standards and what they mean for audit functions and audit committees.

Part 2, Managing risk, shows how to build a risk register that actually informs decisions, including the known weaknesses of the familiar heat map, and explains operational resilience under APRA's CPS 230 with lessons for organisations outside its reach.

Part 3, Risks on the board agenda, examines what the data says about occupational fraud and how to control it, the mandatory climate reporting and assurance regime, and cyber risk from a director's point of view.

How to read RiskWise

We explain standards and laws in plain English and date every reference, because requirements change. Our articles are a starting point, not a substitute for the standard itself, the legislation, the regulator's guidance or professional advice. Where something is our view, we say so.

Good assurance is quiet. When it works, nothing dramatic happens. We hope this magazine helps keep it that way.

Thank you for reading the first RiskWise.

Warm regards,
Sukh Sandhu
Editor-in-Chief, RiskWise

PART 1

Assurance foundations

The Three Lines Model and the new Global Internal Audit Standards.

ASSURANCE

The Three Lines Model Explained: Who Owns Risk, Who Checks It, and Who Tells the Board

By Sukh Sandhu

The Three Lines Model is the most widely quoted picture of how an organisation divides responsibility for risk, yet it is also one of the most misread. This article sets out what the Institute of Internal Auditors actually says, from the 2020 model to the revised Statement of Position issued in July 2026, and shows how a mid-sized Australian organisation can put it to work without building a bureaucracy.

Why a diagram became a governance standard of sorts

Every organisation faces the same basic question: if something goes wrong, who should have stopped it, who should have noticed, and who should have told the board? Boards cannot run operations themselves. They delegate authority to management and then need some way of knowing that the delegation is working. The Three Lines Model is an answer to that problem.

The model began life as the "Three Lines of Defense". The Institute of Internal Auditors (IIA) popularised that version in a 2013 position paper, and regulators and banks took it up enthusiastically after the global financial crisis. The defensive framing was intuitive: operational managers were the first line of defence, risk and compliance specialists the second, and internal audit the third.

In July 2020 the IIA replaced it with the Three Lines Model. The change of name was deliberate. Commentators at the time noted that the IIA wanted to move away from the idea of risk management as purely defensive and towards the idea that good governance both creates and protects value. The 2020 model also gave the governing body a much more prominent place in the picture and loosened the rigid boundaries between the lines.

The latest step came on 8 July 2026, when the IIA published a revised Statement of Position titled *Assurance and Advice in Support of Effective Governance: Three Lines Model*. The IIA says the model's core structure is unchanged, but the revision sharpens the language on independence, distinguishes assurance from advice, and gives practical guidance on overlapping roles and outsourcing.

> *The Three Lines Model is guidance, not law. It is a principles-based framework that organisations adapt to their own size, sector and regulatory obligations.*

The roles in plain language

The model describes a small number of parties and how they relate to one another. The 2026 statement uses the word "board" for every kind of governing body, including a board of directors, a board of governors or trustees, or a group of elected officials, and, where none of these exists, the group or person that acts as the organisation's highest-level board.

The governing body

The board is accountable to stakeholders for the organisation's oversight. In the 2020 model, the governing body ensures that appropriate structures and processes are in place, delegates responsibility and provides resources to management, sets the organisation's appetite for risk, and oversees internal audit. The 2026 statement restates this simply: boards set purpose, risk appetite and expectations, and oversee the pursuit of strategic objectives.

Crucially, the board does not sit outside the model as an audience. It is part of the model. It decides how much separation it wants between the lines, approves the internal audit charter, and decides whether the assurance it receives is enough.

Management: the first line

First line roles belong to the people who deliver products and services and support them. The 2026 statement says the first line owns and manages risks and is responsible for the design and operation of processes and controls. It supervises activities, monitors performance and may run control self-assessments.

One clarification often surprises people. The IIA counts "back office" functions such as human resources, administration and building services as first line activities when they are doing their ordinary work. Second line roles are the complementary activities focused specifically on risk.

Management: the second line

Second line roles provide specialist expertise, support, monitoring and challenge. Typical examples are an enterprise risk function, a compliance team, a work health and safety adviser, an information security team or a privacy officer. The 2026 statement notes that the second line is still part of management, but often brings a perspective independent of the first line reporting hierarchy.

The second line's strength is specialist knowledge and closeness to the business. Its limitation, as the IIA candidly lists, is that reporting through management can impair it and it may focus on procedural compliance rather than deep assurance.

Internal audit: the third line

The internal audit function provides independent and objective assurance on governance, risk management, compliance and control, and advice without taking on management responsibility. It reports functionally to the board, usually through an audit committee, and administratively to the chief executive.

The 2026 statement describes internal audit as the "integrator of assurance". Because it reports to the board and can look across the whole organisation, it is the line best placed to tell the board whether the first and second lines are working together as a system, not just whether individual controls work.

External assurance providers

External auditors, regulators, accreditation bodies and certification auditors sit outside the three lines. The 2026 statement notes that external auditors provide assurance mainly to outside stakeholders on financial statements and other required disclosures, while regulatory inspections help enforce mandatory standards. Their work can be useful to the organisation, but it is not a substitute for internal assurance.

The principles: 2020 and 2026

The 2020 model was built on six principles. The 2026 Statement of Position restates the foundations as five principles. Both versions are worth knowing, because most organisational policies, training material and regulator documents still refer to the 2020 wording.

Principle	2020 model (six principles)	2026 statement (five principles)
1	Governance needs structures and processes for accountability, action and assurance	Boards set purpose, risk appetite and expectations
2	Governing body roles: oversight, delegation, stakeholder alignment	Oversight depends on reliable, balanced information
3	Management and first and second line roles	Board and senior management define roles and accountability
4	Third line roles: independent assurance and advice	Distinct sources of assurance, including an independent one
5	Third line independence from management	Advice complements assurance
6	Creating and protecting value through alignment	(Value creation runs through the whole statement)

The 2020 principles focused on describing roles. The 2026 principles focus on what the board needs: purpose, reliable information, clear accountability, independent assurance and useful advice. In our view, that shift is the most important thing for directors to notice. The model is increasingly written for boards rather than for auditors.

What changed in 2026

The revised statement does not redraw the diagram, but it adds substance in five areas.

1. **Independence explained.** The IIA lists the essential elements of independence: reporting lines and authority to escalate, autonomy over scope and planning, unrestricted access to information and people, control over resources, and protection from retaliation. It warns that independence should not become isolation.

2. **Assurance and advice separated.** Assurance confirms whether processes are adequate and effective. Advice identifies emerging issues and opportunities. Both are delivered across all three lines, with different depth and safeguards.
3. **A cooling-off period.** The statement says a period of at least 12 months between responsibility for a process or decision and providing assurance over it is typically sufficient to safeguard objectivity.
4. **Coordination and reliance.** The statement encourages assurance maps, shared risk taxonomies, aligned reporting and coordinated planning. It describes "integrated assurance" as a more mature form of coordination, while making clear it is not a structural requirement.
5. **Overlaps and outsourcing.** It addresses situations where internal audit performs second line work or where the chief audit executive supervises a compliance function, and it states plainly that outsourcing an activity does not change its place in the model or the board's accountability for it.

Applying the model in a mid-sized Australian organisation

Most writing about the Three Lines Model assumes a bank with hundreds of risk staff. Most Australian organisations look nothing like that. Consider a typical mid-sized business, not-for-profit or member organisation with 150 to 800 staff, a board of six to nine directors, one or two risk or compliance staff, and an internal audit function that is either a small in-house team or an outsourced provider.

The 2026 statement explicitly recognises this reality. It says there is no single structure that fits every organisation, and that the need for separate first, second and third line roles depends largely on the nature and magnitude of risks and any regulatory obligations. Below is a practical way to apply the model in that setting.

Step 1: Write down who owns what

Start with your top ten to fifteen enterprise risks. For each one, name the executive who owns it (first line), the specialist who supports and challenges it (second line, if any), and whether internal audit has looked at it in the last three years (third line). This single page is the beginning of an assurance map.

Step 2: Decide where you genuinely need a second line

A mid-sized organisation rarely needs a large second line, but it usually needs at least some specialist challenge in areas where the consequences of failure are severe or the rules are technical. Common candidates are work health and safety, privacy and cyber security, financial controls, and any sector-specific regulation such as aged care, education, health or financial services. Where there is no dedicated person, consider whether an external adviser can provide periodic challenge, and record who engages and directs that adviser.

Step 3: Make internal audit's mandate explicit

Whether internal audit is in-house or outsourced, it needs a board-approved charter, a direct line to the audit and risk committee, unrestricted access to records and people, and a risk-based plan. The 2026 statement says outsourced providers should be categorised

according to the function that engages and directs them. In practice, that means an outsourced internal auditor who is engaged and directed by the chief financial officer is not functioning as the third line, however good the work.

Step 4: Manage overlaps openly

Small teams mean overlaps are almost inevitable. The head of internal audit may also run the risk register, or the risk manager may be asked to perform compliance testing. The IIA does not prohibit these arrangements in most settings, but it expects safeguards. Drawing on the 2026 statement, these include:

- documenting the allocation of responsibilities, for example in the internal audit charter
- full disclosure to the board of any second line responsibility taken on by internal audit, and the risks it creates
- arranging for another independent party to provide assurance over any area where internal audit has operational responsibility
- separating advisory work clearly from later assurance work
- board approval of any expanded remit for the chief audit executive

Step 5: Report to the board as one picture

The model only adds value if the board sees a coherent view. A combined assurance report, produced once or twice a year, can show each major risk, its owner, the second line activity over it, the most recent internal audit result and any external assurance. Gaps and duplications become visible immediately.

One risk, three lines: an illustration

It helps to see the model applied to a single risk. Take payment fraud through fraudulent changes to supplier bank details, a common scheme in which a criminal impersonates a supplier and asks for payments to be redirected. In a hypothetical mid-sized organisation, the lines might look like this.

Line	Who	What they do
First	Accounts payable team and finance manager	Verify every bank detail change by calling the supplier on a known number; review exception reports
Second	Financial controller or risk and compliance officer	Set the verification policy, run awareness training, sample changes each quarter and report trends
Third	Internal audit (in-house or outsourced)	Test the design and operation of the controls periodically and report independently to the committee
External	External auditor	Considers payment controls as part of the financial report audit, for its own purpose

Each line asks a different question. The first line asks whether today's payments are correct. The second asks whether the control framework is working across the organisation and whether the policy remains fit for purpose. The third asks whether the

board can rely on both. If any line is missing, the gap is visible on one page, and the board can decide whether to accept it.

Australian context

For listed entities, Recommendation 7.3 of the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* (4th edition) asks entities to disclose whether they have an internal audit function, how it is structured and what role it performs, or, if not, how they evaluate and continually improve the effectiveness of their governance, risk management and internal control processes. Recommendation 7.2 asks the board or a committee to review the risk management framework at least annually. A draft 5th edition was released for consultation in July 2026, with submissions closing in September 2026; at November 2026 the 4th edition remains the operative version. Regulated sectors such as banking, insurance and superannuation have additional prudential requirements that shape how the lines are organised.

Common misunderstandings

The model's simplicity is both its strength and its weakness. These are the misreadings that recur most often.

"The lines are a sequence of defences"

The old defence metaphor suggested that risk passes the first line, then the second, then the third, like a ball passing defenders. In reality the lines work at the same time and on different questions. Internal audit is not a final safety net that catches what management misses. If an organisation is relying on internal audit to find errors, its first line controls are not doing their job.

"Risk management belongs to the risk team"

The first line owns risk. The second line helps, monitors and challenges, but it does not own the risks of the business. When a risk manager becomes the de facto owner of every risk, accountability blurs and line managers disengage.

"Internal audit must never give advice"

The IIA has always recognised advisory work, and the 2026 statement treats advice as complementary to assurance. The safeguards are clear roles, no management decisions by the adviser, and informing the board of the nature and scope of advisory work.

"Independence means distance"

The 2026 statement explicitly warns that independence should not be interpreted as isolation. An internal audit function that refuses to talk to the risk team, or a risk team that refuses to share information with audit, is not more independent. It is less useful.

"The model prescribes an organisation chart"

It does not. The IIA describes the document as principles-based and says it does not prescribe organisational structures. Two well-governed organisations can implement the model very differently.

"Outsourcing transfers responsibility"

Outsourcing internal audit, payroll, information technology or a compliance review does not transfer accountability. The 2026 statement is explicit that outsourcing does not change the activity's role in the model or the board's accountability for it.

"External audit covers us"

The external auditor's statutory focus is the financial report. It does not provide assurance over operational risk, culture, cyber security or strategy unless separately engaged to do so, and even then it is assurance for a defined purpose.

A quick diagnostic for directors

Directors can test whether their organisation's lines are working by asking a few direct questions at the next audit and risk committee meeting.

Question	Healthy answer	Warning sign
Who owns our top five risks?	Named executives who can describe their controls	"The risk team looks after that"
What does the second line actually challenge?	Specific examples of pushback in the past year	Only templates and reminders
Does internal audit report to us directly?	Yes, with private sessions without management	Only through the CFO
Where do the lines overlap?	Documented, with safeguards	Nobody has thought about it
Do we have an assurance map?	Yes, reviewed at least annually	No single view of coverage

What to do this month

1. List your top ten risks and name the first line owner, second line support and last internal audit coverage for each.
2. Read your internal audit charter against the 2026 Statement of Position and check that reporting lines, access and resourcing are clear.
3. Identify any area where internal audit has operational responsibility and decide who else provides assurance over it.
4. Ask management to prepare a one-page combined assurance view for the next committee meeting.
5. Schedule a private session between the committee and the head of internal audit, without management present.
6. Check whether your policies still describe "three lines of defence" and update the language and role descriptions where needed.

The bottom line

The Three Lines Model has survived more than a decade because it gives boards and managers a common vocabulary. Its value does not come from the diagram. It comes from honest answers to three questions: who owns the risk, who challenges the owner, and who gives the board an independent view. The 2026 update pushes those questions firmly onto the board's agenda. In our view, mid-sized organisations that answer them

clearly on one page will be better governed than many larger organisations with far more elaborate structures.

Sources

- The Institute of Internal Auditors, Assurance and Advice in Support of Effective Governance: Three Lines Model, Statement of Position, July 2026, https://www.theiia.org/globalassets/site/resources/statements-of-position/tlm_assurance_advice_support_effective_gov_en.pdf
- The Institute of Internal Auditors, Statements of Position (Three Lines Model and Role of the Internal Audit Function in Enterprise Risk Management, published 8 July 2026), https://www.theiia.org/en/resources/statements-of-position/
- The Institute of Internal Auditors, The IIA's Three Lines Model: An Update of the Three Lines of Defense, July 2020, https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf
- Journal of Accountancy, 3 lines of defense model for risk management gets major update, July 2020, https://www.journalofaccountancy.com/news/2020/jul/3-lines-of-defense-model-for-risk-management-gets-major-update/
- Mayer Brown, The Blurred Lines of Organizational Risk Management, 31 July 2020, https://www.mayerbrown.com/en/perspectives-events/publications/2020/07/the-blurred-lines-of-organizational-risk-management/
- CRI Advisors, The IIA Updates Its Statement of Position on the Three Lines Model, 27 August 2026, https://www.criadv.com/insight/iia-three-lines-model-update/
- ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, February 2019, https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/cgc-principles-and-recommendations-fourth-edn.pdf
- Australian Institute of Company Directors, ASX releases draft 5th edition Corporate Governance Principles and Recommendations, July 2026, https://www.aicd.com.au/good-governance/asx-corporate/corporate-governance-principles-5th-draft-edition.html

ASSURANCE

The Global Internal Audit Standards: What Changed, What Is Now Mandatory, and What Boards Should Ask

By Sukh Sandhu

The Global Internal Audit Standards replaced the profession's 2017 rulebook and have applied since 9 January 2025. Nearly two years on, they are being joined by a growing set of mandatory topical requirements, starting with cybersecurity. This guide explains the structure, the real changes, the quality assessment regime and the questions every audit committee should now be asking.

Why the Standards matter beyond the audit team

Internal audit standards can sound like a technical matter for the profession. They are not. The Global Internal Audit Standards, issued by the Institute of Internal Auditors (IIA), now set out in mandatory terms what boards and senior management must do to support an effective internal audit function. For the first time, a significant part of the rulebook is about the board, not the auditor.

For Australian directors, this matters in three ways. First, many internal audit functions, whether in-house or outsourced, claim conformance with the IIA Standards, and that claim should mean something. Second, the Standards change what a board can reasonably expect to receive from internal audit. Third, they give directors a structured basis for evaluating the function they oversee.

The timeline

Date	Event
9 January 2024	IIA releases the Global Internal Audit Standards
9 January 2025	Standards become effective, replacing the 2017 Standards
5 February 2025	Cybersecurity Topical Requirement issued
5 February 2026	Cybersecurity Topical Requirement effective
15 September 2026	Third-Party Topical Requirement effective
15 December 2026	Organizational Behavior Topical Requirement effective
30 April 2027	Organizational Resilience Topical Requirement effective

The Standards were published a year before they took effect, giving functions a transition year in which the 2017 Standards remained valid. Topical requirements follow a similar pattern: the IIA's general approach is that each becomes effective about twelve months after it is issued.

How the Standards are built

The Standards are organised into five domains, 15 principles and 52 individual standards. Each standard sets out requirements, considerations for implementation and examples of evidence of conformance. This is a significant change in format. Under the 2017 framework, mandatory standards and recommended implementation guidance sat in separate documents. Now much of the practical guidance sits alongside the requirement itself.

The five domains and 15 principles

Domain	Principles
I. Purpose of Internal Auditing	A purpose statement (no numbered principles)
II. Ethics and Professionalism	1 Demonstrate integrity; 2 Maintain objectivity; 3 Demonstrate competency; 4 Exercise due professional care; 5 Maintain confidentiality
III. Governing the Internal Audit Function	6 Authorized by the board; 7 Positioned independently; 8 Overseen by the board
IV. Managing the Internal Audit Function	9 Plan strategically; 10 Manage resources; 11 Communicate effectively; 12 Enhance quality
V. Performing Internal Audit Services	13 Plan engagements effectively; 14 Conduct engagement work; 15 Communicate engagement results and monitor action plans

Domain I replaces the previous Mission, Definition and Core Principles with a single statement of purpose. In broad terms, it describes internal audit as strengthening the organisation's ability to create, protect and sustain value by providing the board and management with independent, risk-based and objective assurance, advice, insight and foresight.

Domain II absorbs what was previously a separate Code of Ethics. Ethics is now part of the Standards rather than a document alongside them.

The "must" and the "should"

The Standards use deliberate language. Requirements use "must". Considerations for implementation describe common and preferred practices. Under Standard 4.1, if laws or regulations prohibit conformance with any part of the Standards, conformance with all other parts is still required and appropriate disclosures must be made. Where internal auditors are unable to conform with a requirement for other reasons, the chief audit executive must document and communicate the circumstance, the alternative actions taken, their impact and the rationale. In practice, this means a claim of conformance should always be read together with any disclosed exceptions.

The key changes from the 2017 framework

The IIA describes the 2024 Standards as an evolution, but several changes are substantial.

1. Essential conditions for the board and senior management

Domain III contains a new concept: essential conditions. These set out what the board and senior management are expected to do so that internal audit can be effective. They include approving the internal audit charter, supporting the function's mandate, ensuring the chief audit executive has direct and unrestricted access to the board, approving the internal audit plan and budget, and overseeing the function's quality.

Professional standards cannot compel a board to do anything. Instead, the Standards place the obligation on the chief audit executive: if the board or senior management disagrees with an essential condition, the chief audit executive must explain, with examples, how its absence may affect the function's ability to fulfil its purpose or conform with the Standards. In our view, this is the most important change for directors. It invites a direct conversation about whether the board is giving internal audit what it needs.

2. A formal mandate

The Standards distinguish between the internal audit mandate, which is the authority, role and responsibilities given to the function by the board or by law, and the charter, which documents it. The board is expected to approve the charter and review it periodically.

3. An internal audit strategy

Standard 9.2 requires the chief audit executive to develop and implement a strategy for the function that supports the organisation's objectives, including a vision, strategic objectives and supporting initiatives, and to review it with the board periodically. Many functions previously produced only an annual plan.

4. Coordination and reliance

Standard 9.5 requires the chief audit executive to coordinate with other internal and external assurance providers and to consider relying on their work. Where internal audit relies on another provider, the chief audit executive must document the basis for that reliance and remains responsible for internal audit's conclusions. The implementation guidance suggests evaluating the other provider's independence, competency, objectivity and due professional care. This links directly to the Three Lines Model's emphasis on integrated assurance.

5. Performance measurement

Standard 12.2 requires the chief audit executive to develop performance objectives for the function, taking account of the board's and senior management's expectations, and a methodology for measuring progress against them. Under the essential conditions in Standard 8.3, the board is expected to approve those performance objectives at least annually. Boards should expect to see measures of the function's effectiveness, not just counts of audits completed.

6. Prioritised findings and engagement conclusions

In Domain V, Standard 14.3 requires internal auditors to evaluate each finding's significance, considering likelihood and impact, and to prioritise findings using methodologies set by the chief audit executive. Standard 14.5 requires an engagement conclusion, and for assurance engagements that conclusion must include a judgment on the effectiveness of the processes reviewed, including an acknowledgment when processes are effective. Clear ratings and conclusions make it easier for boards to compare results over time.

7. Communicating risk acceptance

Standard 11.5 addresses the situation where management accepts a level of risk that the chief audit executive believes exceeds the organisation's risk appetite or tolerance. The chief audit executive must discuss the matter with senior management and, if it is not resolved, communicate it to the board. This gives a formal path for one of the hardest conversations in governance.

8. Consulting becomes advisory

The term "consulting services" has been replaced with "advisory services". The substance is similar, but the language aligns with the IIA's broader positioning of assurance and advice as complementary.

Topical requirements: a new mandatory layer

The most significant development since the Standards took effect is the arrival of topical requirements. These are mandatory components of the IIA's International Professional Practices Framework that set a minimum baseline for how internal auditors address specific risk areas.

How they apply

Topical requirements are not a requirement to audit every topic every year. Their application depends on the internal audit function's risk assessment. According to the IIA, internal auditors must apply a topical requirement, in conformance with the Standards, when providing assurance services on that topic. For advisory work on a topic, applying it is recommended rather than required. Where an internal audit function decides that parts of a topical requirement do not apply to a particular engagement, it should document the rationale. External quality assessments carried out after a topical requirement's effective date will assess conformance with it.

Cybersecurity

The Cybersecurity Topical Requirement was issued on 5 February 2025 and became effective on 5 February 2026. It provides a consistent approach for assessing the design and implementation of cybersecurity governance, risk management and control processes. In practical terms, when internal audit provides assurance over cyber security, it must cover a minimum set of matters across those three areas rather than, for example, testing a handful of technical controls in isolation.

Third parties

The Third-Party Topical Requirement was issued on 15 September 2025 and became effective on 15 September 2026. It addresses the governance, risk management and controls over third-party relationships. For Australian organisations that depend on outsourced technology, payroll, logistics or professional services, it overlaps substantially with prudential expectations such as APRA's operational risk standard.

What is coming

At November 2026, the IIA lists an Organizational Behavior Topical Requirement effective 15 December 2026 and an Organizational Resilience Topical Requirement effective 30 April 2027. It also lists a Talent Management Topical Requirement scheduled for public consultation in January 2027 and an Anti-Corruption Topical Requirement scheduled to be issued in the fourth quarter of 2026. Audit committees should expect the internal audit plan to show which topical requirements are in scope and why.

Topical requirement	Effective	Typical audit committee question
Cybersecurity	5 February 2026	When did we last get assurance over cyber governance, not just technical controls?
Third-Party	15 September 2026	Which suppliers could stop our critical services, and who oversees them?
Organizational Behavior	15 December 2026	How does internal audit form a view on culture and conduct?
Organizational Resilience	30 April 2027	Has our ability to recover from severe disruption been tested?

Quality assessment

Standard 8.3 (Quality), Standard 8.4 and Principle 12 (Enhance Quality) set out how the quality of an internal audit function is assured.

Internal assessments

The chief audit executive must maintain a quality assurance and improvement program that includes internal assessments, made up of ongoing monitoring and periodic self-assessments, and external assessments. At least annually, the results of internal quality assessment must be communicated to the board and senior management, covering conformance with the Standards and achievement of performance objectives.

External quality assessments

Standard 8.4 requires an external quality assessment at least once every five years by a qualified, independent assessor or assessment team. The requirement may also be met through a self-assessment with independent validation. At least one person on the assessment team must hold an active Certified Internal Auditor designation. The chief audit executive must develop a plan for the assessment and discuss it with the board.

The Standards place a direct expectation on the board here. Under the essential conditions in Standard 8.4, the board is expected to review and approve the assessment plan,

including its scope, frequency, the assessors' competence and independence, and the rationale for any choice of self-assessment with independent validation. The board should receive the complete results directly from the assessor, approve action plans and monitor progress. In our view, a function cannot credibly claim to conform with the Standards unless its quality program supports that claim.

What a good assessment report tells you

A useful external quality assessment report should show an overall conformance rating, ratings by principle or standard, specific gaps, and a practical improvement plan. It should also comment on stakeholder perception and on whether the function is adding value. Directors should be wary of reports that consist mainly of a pass mark with little explanation.

Applying the Standards in Australia

The Global Internal Audit Standards are the professional standards of a global membership body. They are not Australian law. Their influence in Australia comes through several routes:

- IIA Australia promotes the Standards to its members and supports their adoption locally.
- Many internal audit charters, both in the private sector and across government, commit the function to conform with the IIA Standards.
- Outsourced internal audit providers typically state in their engagement terms that their work is performed in accordance with the IIA Standards.
- Regulators in some sectors expect internal audit functions to operate in line with recognised professional standards, even where they do not name the IIA directly.

For listed entities, Recommendation 7.3 of the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* asks entities to disclose whether they have an internal audit function, how it is structured and what role it performs. The Standards give boards a benchmark for answering that question with substance.

What audit committees should ask

The following questions are designed for an audit and risk committee meeting. They are drawn directly from the structure of the Standards.

On mandate and positioning

1. Has the board approved the internal audit charter in the last year, and does it reflect the mandate, scope and types of services we actually want?
2. Does the chief audit executive have direct, unrestricted access to the committee, including private sessions without management present?
3. Who approves the chief audit executive's appointment, removal, remuneration and performance review?
4. Has the chief audit executive told us about any essential condition that is not in place, and what the effect is?

On strategy and resources

1. Do we have a documented internal audit strategy, and when did we last discuss it?
2. Is the function adequately resourced for the plan we approved, including specialist skills in technology, cyber security and data analytics?
3. Which assurance providers does internal audit rely on, and how does it evaluate their work?

On topical requirements

1. Which topical requirements are relevant to our risk profile, and how does the current plan address them?
2. If cyber security or third-party risk is not in this year's plan, what is the documented rationale?

On reporting

1. Are findings rated consistently, and can we see trends across engagements over several years?
2. Has management accepted any risk that the chief audit executive believes exceeds our risk appetite?
3. Does internal audit give us themes and insights across engagements, not just a list of individual reports?

On quality

1. When was our last external quality assessment, who performed it and what was the result?
2. Did we see the full report and the action plan, and have the actions been closed?
3. How does internal audit measure its own performance, and what do the measures show?

A conformance checklist for the chief audit executive

For internal audit leaders, the following checklist is a practical starting point for a self-assessment against the Standards and topical requirements.

- Charter approved by the board, reflecting the mandate and the purpose statement
- Essential conditions discussed with the board and senior management, with gaps documented
- Independence and reporting lines confirmed and documented
- Internal audit strategy approved and reviewed
- Risk-based plan that addresses relevant topical requirements, with documented rationale for exclusions
- Coordination and reliance approach documented, including an assurance map
- Methodologies updated for prioritised findings and engagement conclusions
- Process for escalating risk acceptance that exceeds appetite
- Performance measures agreed with the board
- Quality assurance and improvement program with ongoing monitoring and periodic self-assessment

- External quality assessment scheduled within five years, with at least one assessor holding an active Certified Internal Auditor designation

What to do this month

1. Ask the chief audit executive for a one-page summary of conformance with the Standards, including any disclosed departures.
2. Confirm the date and outcome of the last external quality assessment and schedule the next one if it falls within the next eighteen months.
3. Review the internal audit plan against the four issued topical requirements and record which are in scope.
4. Put the internal audit strategy and performance measures on the next committee agenda.
5. Hold a private session with the chief audit executive to discuss whether any essential condition is missing.

The bottom line

The Global Internal Audit Standards make internal audit's relationship with the board more explicit than ever. They ask more of auditors, but they also ask more of directors: a clear mandate, real access, adequate resources and genuine interest in quality. The arrival of mandatory topical requirements means the content of internal audit work is also becoming more standardised. In our view, the boards that benefit most will be those that treat the Standards not as the audit team's compliance exercise, but as a framework for deciding what kind of assurance they need.

Sources

- The Institute of Internal Auditors, Global Internal Audit Standards, 2024 edition, https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/
- The Institute of Internal Auditors, Issued and upcoming Topical Requirements, accessed November 2026, https://www.theiia.org/en/standards/2024-standards/topical-requirements/
- The Institute of Internal Auditors, Cybersecurity Topical Requirement (issued 5 February 2025, effective 5 February 2026), https://www.theiia.org/en/standards/2024-standards/topical-requirements/cybersecurity
- The Institute of Internal Auditors, Third-Party Topical Requirement (issued 15 September 2025, effective 15 September 2026), https://www.theiia.org/en/standards/2024-standards/topical-requirements/third-party/
- Plante Moran, The IIA's topical requirements: a new baseline, October 2026, https://www.plantemoran.com/explore-our-thinking/insight/2026/10/iias-topical-requirements-new-baseline
- KPMG, IIA Topical Requirements for internal auditing, https://kpmg.com/be/en/insights/risk/iia-topical-requirements-for-internal-auditing.html

- KPMG, Global Internal Audit Standards, 2024, https://kpmg.com/us/en/articles/2024/global-internal-audit-standards.html
- Baker Tilly, Preparing for an external quality assessment under the Global Internal Audit Standards, https://www.bakertilly.com/insights/preparing-external-quality-assessment-under-global-internal-audit-standards
- Armanino, Changes to the internal audit IPPF and how to prepare, https://www.armanino.com/articles/changes-to-internal-audit-ippf-how-to-prepare/
- ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, February 2019, https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/cgc-principles-and-recommendations-fourth-edn.pdf

PART 2

Managing risk

Risk registers that inform decisions, and operational resilience under CPS 230.

MANAGING RISK

Building a Risk Register That Works: From ISO 31000 to the Boardroom

By Sukh Sandhu

Almost every Australian organisation has a risk register, and many of them are rarely read, seldom updated and almost never used to make a decision. This article explains what the international standard actually asks for, why the familiar likelihood and consequence matrix is weaker than it looks, and how to build a register, with owners and controls, that a board can genuinely use.

The problem with most risk registers

Risk registers tend to fail in predictable ways. They grow to hundreds of lines. Risks are described as vague nouns such as "cyber" or "reputation". Ratings stay the same for years. Controls are listed but never tested. Owners are departments rather than people. The register is updated the week before the audit and risk committee meets and then filed away.

None of this is required by any standard. The international guidance on risk management is short, principles-based and focused on decisions. The gap is not in the guidance but in how it is applied.

What ISO 31000:2018 actually says

ISO 31000:2018 *Risk management: Guidelines* is the international standard most Australian organisations use as their reference point. It has been adopted in Australia as AS ISO 31000:2018. It is a guideline, not a certifiable requirements standard, which means organisations cannot be certified against it. At November 2026, the 2018 edition remains current, although a third edition is in development within ISO's risk management technical committee.

ISO 31000 defines risk as the "effect of uncertainty on objectives". That definition matters. Risk is not simply a bad thing that might happen; it is the effect uncertainty has on what the organisation is trying to achieve. A register that is not linked to objectives has already missed the point.

The standard is built on three parts: principles, a framework and a process.

The principles

ISO 31000 places the creation and protection of value at the centre and lists eight principles that describe effective risk management.

Principle	What it means in practice

Principle	What it means in practice
Integrated	Risk management is part of all activities, not a separate exercise
Structured and comprehensive	A consistent approach produces comparable results
Customised	The framework fits the organisation's context and objectives
Inclusive	Stakeholders are involved at the right time
Dynamic	Risks change and the approach responds
Best available information	Inputs use historical and current information and future expectations, with limitations acknowledged
Human and cultural factors	Behaviour and culture influence every stage
Continual improvement	Risk management improves through learning and experience

The framework

The framework is the organisational arrangements that make risk management work. ISO 31000 describes leadership and commitment at the centre, surrounded by five components: integration, design, implementation, evaluation and improvement. In plain terms, the board and executive must sponsor it, it must be built into how decisions are made, it must be designed for the organisation, put into practice, checked and improved.

The process

The risk management process is the part most people recognise. It has six elements:

1. **Communication and consultation** with stakeholders throughout.
2. **Scope, context and criteria**, including the criteria used to decide how significant a risk is.
3. **Risk assessment**, made up of risk identification, risk analysis and risk evaluation.
4. **Risk treatment**, selecting and implementing options to address risk.
5. **Monitoring and review** of the process and its outcomes.
6. **Recording and reporting**, so that results are documented and communicated.

The risk register belongs mainly in the last of these: it is the record. But a register can only be as good as the context, criteria and assessment behind it.

Risk appetite and tolerance

A register without an appetite statement is a list without a yardstick. If the board has not said how much risk it is willing to take, nobody can say whether a residual rating is acceptable.

Definitions

The terms are used loosely, so it helps to anchor them to published sources.

- ISO's risk management vocabulary, first in ISO Guide 73:2009 and now in ISO 31073:2022, which superseded it, describes risk appetite as the amount and type of risk an organisation is willing to pursue or retain.
- COSO's 2017 framework, *Enterprise Risk Management: Integrating with Strategy and Performance*, describes risk appetite as the types and amount of risk, on a broad level,

an organisation is willing to accept in pursuit of value. It treats tolerance as the acceptable variation in performance relative to objectives.
- The IIA's Global Internal Audit Standards also use both terms and expect the chief audit executive to escalate to the board where management accepts risk that exceeds appetite or tolerance.

Making appetite usable

A useful appetite statement has three layers.

1. **Qualitative statements by risk category.** For example: "We have no appetite for serious harm to people", "We have a low appetite for breaches of privacy law", "We have a moderate appetite for investment in new services".
2. **Measurable tolerances.** For example: lost time injury frequency below a stated rate, no notifiable data breaches, liquidity coverage above a stated number of months of operating costs.
3. **Escalation triggers.** For example: any risk rated high after controls must be reported to the audit and risk committee with a treatment plan.

In our view, the second layer is where most organisations fall short. Without numbers, appetite statements become statements of values, which are worthwhile but do not help anyone decide whether a risk is within bounds.

Likelihood and consequence matrices, and their weaknesses

The five by five matrix, with likelihood on one axis and consequence on the other, is the most common tool in Australian risk registers. It is quick, familiar and easy to communicate. It is also less reliable than its widespread use suggests.

What the research shows

The best known critique is Louis Anthony Cox Jr's paper "What's Wrong with Risk Matrices?", published in *Risk Analysis* in 2008. Cox examined the mathematical properties of risk matrices and identified four main limitations.

- **Poor resolution.** Typical matrices can reliably compare only a small fraction of randomly selected pairs of hazards. They can give identical ratings to risks that differ greatly in size, a problem he calls range compression.
- **Errors.** Matrices can assign higher ratings to quantitatively smaller risks. Where frequency and severity are negatively correlated, Cox showed they can perform worse than random.
- **Suboptimal resource allocation.** Matrix categories do not, on their own, tell you how best to spend money on reducing risk.
- **Ambiguous inputs and outputs.** Severity is hard to categorise objectively when consequences are uncertain, and different users can rate the same risk very differently.

Cox did not argue that matrices should never be used. His conclusion was that they should be used with caution and with clear explanations of the judgments built into them.

Other researchers have reached similar conclusions. Douglas Hubbard and Dylan Evans, writing in the *IBM Journal of Research and Development* in 2010, examined scoring methods and ordinal scales and argued that they can introduce errors and give a false sense of precision. Philip Thomas, Reidar Bratvold and J. Eric Bickel, in a 2014 paper in *SPE Economics and Management*, reviewed risk matrices used in the oil and gas industry and identified problems including ranking reversals, where the ranking of risks changes depending on how the scale is designed.

Practical responses

The answer for most organisations is not to abandon the matrix but to use it more carefully.

1. **Define scales in numbers where you can.** "Likely" should mean a stated probability range over a stated period. "Major" consequence should be defined in dollars, people affected, days of disruption or regulatory outcomes.
2. **Rate consequence against objectives.** Use the same consequence categories that appear in the appetite statement.
3. **Do not multiply ordinal scores.** A score of 4 multiplied by 5 is not twice as risky as 2 multiplied by 5. Treat cells as categories, not arithmetic.
4. **Record the reasoning.** A short sentence explaining the rating is worth more than the colour of the cell.
5. **Quantify the few risks that matter most.** For the top handful of risks, a simple range estimate of financial impact or a scenario analysis gives the board far more insight than a heat map.
6. **Calibrate.** Ask several people to rate the same risk independently and discuss differences. Wide disagreement is information.

Controls and owners

Owners must be people

Every risk needs a named owner, normally an executive, who is accountable for managing it. Every control needs a named control owner, who may be a different person, responsible for operating it. An owner of "Finance" or "IT" is not an owner.

Describe controls precisely

A good control description answers five questions: what is done, by whom, how often, using what evidence, and what happens when an exception is found. "Monthly reconciliation" is not a control description. "The financial controller reconciles the bank accounts to the general ledger monthly, documents the reconciliation in the finance system and escalates unreconciled items over a stated threshold to the chief financial officer" is.

Distinguish types of control

Classifying controls helps reveal gaps.

Type	Purpose	Example
Preventive	Stop an event from happening	Two-person approval of

Type	Purpose	Example
		supplier bank changes
Detective	Identify an event that has happened	Exception report on duplicate payments
Corrective	Limit the impact after an event	Tested data backup and restoration
Directive	Guide behaviour	Code of conduct and training

A risk managed only by directive controls, such as policies and training, is usually weaker than it appears.

Rate control effectiveness, then test it

Many registers show a residual rating that depends on controls nobody has tested. Each key control should carry an effectiveness rating and a date of the last test, whether by management self-assessment, the second line or internal audit.

A worked example

The following example is illustrative. It shows part of a register for a hypothetical mid-sized Australian services organisation with about 400 staff, a mix of government and private revenue, and significant reliance on outsourced technology. The organisation uses a five by five matrix with defined scales and a board-approved appetite statement.

Register extract: risks and ratings

ID and risk	Owner	Inherent	Residual	Appetite
R1 Ransomware disrupts client systems for more than 3 days	Chief Information Officer	Extreme	High	Low: outside appetite
R2 Loss of a major government contract at renewal	Chief Executive	High	High	Moderate: at limit
R3 Serious injury to staff working off site	Chief Operating Officer	High	Medium	Nil harm: treatment ongoing
R4 Payment fraud through supplier bank detail changes	Chief Financial Officer	High	Low	Low: within appetite
R5 Failure of the payroll provider	Chief People Officer	High	Medium	Low: outside appetite

Register extract: risk statements

Each line in a register should be written as a statement of cause, event and consequence. For example:

- **R1:** Because of phishing, unpatched systems or a compromised supplier (cause), ransomware encrypts core client systems (event), resulting in more than three days of service outage, client harm, notification obligations under privacy law and contract penalties (consequence).

- **R5:** Because of the provider's financial distress or a technology failure (cause), payroll cannot be processed on time (event), resulting in staff not being paid, breaches of employment obligations and loss of staff trust (consequence).

Register extract: key controls

ID	Key control	Control owner	Type	Last tested
R1	Multi-factor authentication on all remote access	IT Security Manager	Preventive	Internal audit, March 2026
R1	Immutable offline backups, restoration tested quarterly	IT Operations Manager	Corrective	Self-assessment, September 2026
R4	Call-back verification of bank detail changes using known numbers	Accounts Payable Lead	Preventive	Second line, July 2026
R5	Documented manual payroll fallback procedure	Payroll Manager	Corrective	Not yet tested
R3	Lone worker check-in system and site risk assessments	Work Health and Safety Adviser	Preventive	Self-assessment, August 2026

Register extract: treatment plans

ID	Treatment	Owner	Due	Status
R1	Complete endpoint detection rollout and run a ransomware exercise with the executive	Chief Information Officer	February 2027	On track
R2	Client relationship plan and early renewal discussions	Chief Executive	December 2026	On track
R5	Test the manual payroll fallback and review the provider's continuity arrangements	Chief People Officer	January 2027	Overdue start

Several things make this register useful. Every risk is linked to an appetite position, so the board can see immediately that R1 and R5 sit outside appetite. Controls have named owners and test dates, so reliance can be challenged. R5 shows a key control that has never been tested, which is exactly the kind of gap a board should see. Treatment plans have owners and dates.

How to report risk to a board

The register is a management tool. Boards need something different: a concise view that supports decisions. For listed entities, Recommendation 7.1 of the ASX Corporate Governance Council's *Corporate Governance Principles and Recommendations* (4th edition) recommends a board committee to oversee risk, and Recommendation 7.2 recommends that the board or committee review the risk management framework at least annually to satisfy itself that it remains sound and that the entity is operating with due regard to the risk appetite set by the board. Similar expectations apply in practice to many unlisted organisations, not-for-profits and government bodies.

A good board risk report

A board risk report of four to six pages typically covers:

1. **The headline.** Which risks are outside appetite, and what is being done.
2. **Movement.** Which risks have changed rating since the last report and why.
3. **Emerging risks.** New issues that are not yet on the register.
4. **Control assurance.** Which key controls have been tested, by whom, and with what result.
5. **Incidents and near misses.** What happened, what it revealed about controls, and lessons learned.
6. **Treatment progress.** Overdue actions and the reasons.
7. **Key risk indicators.** A small set of trend measures linked to appetite tolerances.

Questions directors should ask

- Which risks are outside appetite, and has the board formally accepted that position or asked for treatment?
- Which key controls have never been independently tested?
- What would a severe but plausible scenario for our top risk cost us, in dollars and days?
- What risks are we taking deliberately in pursuit of strategy, and are they being monitored?
- What did our last significant incident tell us about the accuracy of the register?

> *A risk register is not evidence of risk management. Decisions changed by the register are.*

A checklist for a register that works

- Linked to the organisation's objectives and strategy
- Risks written as cause, event and consequence
- Twenty to forty enterprise risks at most, with operational detail held in lower level registers
- A named executive owner for each risk and a named owner for each key control
- Defined likelihood and consequence scales, in numbers where possible
- Inherent and residual ratings with a short rationale
- A board-approved appetite statement with measurable tolerances
- Control types, effectiveness ratings and last test dates

- Treatment plans with owners, due dates and status
- Key risk indicators for the top risks
- Reviewed by owners at least quarterly and by the board or committee as agreed
- Updated after every significant incident

What to do this month

1. Cut the enterprise register to the risks that genuinely matter to objectives, moving operational detail into business unit registers.
2. Rewrite every risk title as a cause, event and consequence statement.
3. Replace department owners with named executives and named control owners.
4. Check that the likelihood and consequence scales are defined in numbers and match the appetite statement.
5. Identify every key control that has never been tested and agree who will test it.
6. Choose your top three risks and prepare a simple scenario estimate of their financial and operational impact for the board.
7. Redesign the board risk report so the first page shows risks outside appetite.

The bottom line

ISO 31000 asks for something modest and sensible: risk management that is integrated into decisions, tailored to the organisation and continually improved. The risk register is a tool for that purpose, not the purpose itself. In our view, the most useful registers are short, specific and honest about what has and has not been tested, and they use the matrix as a conversation starter rather than a measurement device. A board that can see clearly which risks sit outside appetite, and what is being done about them, is far better placed than one that receives a hundred lines of colour.

Sources

- International Organization for Standardization, ISO 31000:2018 Risk management: Guidelines, February 2018, https://www.iso.org/standard/65694.html
- International Organization for Standardization, ISO 31000 Risk management (overview of principles, framework and process), https://www.iso.org/iso-31000-risk-management.html
- International Organization for Standardization, ISO 31073:2022 Risk management: Vocabulary (supersedes ISO Guide 73:2009), https://www.iso.org/standard/79637.html
- ISO/TC 262, ISO 31000 Risk Management Standard: Time for an Update?, https://committee.iso.org/sites/tc262/home/news/content-left-area/news-and-events-within-iso-tc-26/iso-31000-risk-management-stan-2.html
- Standards Australia, AS ISO 31000:2018 Risk management: Guidelines, https://www.standards.org.au/
- COSO, Enterprise Risk Management: Integrating with Strategy and Performance, June 2017, https://www.coso.org/enterprise-risk-management
- Louis Anthony Cox Jr, What's Wrong with Risk Matrices?, Risk Analysis, vol. 28, no. 2, 2008, pp. 497 to 512, https://doi.org/10.1111/j.1539-6924.2008.01030.x

- Douglas Hubbard and Dylan Evans, Problems with scoring methods and ordinal scales in risk assessment, IBM Journal of Research and Development, vol. 54, no. 3, 2010, https://doi.org/10.1147/JRD.2010.2042914
- Philip Thomas, Reidar B. Bratvold and J. Eric Bickel, The Risk of Using Risk Matrices, SPE Economics and Management, vol. 6, no. 2, 2014, https://doi.org/10.2118/166269-PA
- The Institute of Internal Auditors, Global Internal Audit Standards, Standard 11.5 Communicating the Acceptance of Risks, 2024, https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/
- ASX Corporate Governance Council, Corporate Governance Principles and Recommendations, 4th edition, February 2019, https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/cgc-principles-and-recommendations-fourth-edn.pdf

MANAGING RISK

Operational Resilience and CPS 230: What APRA Requires, and What Every Organisation Can Learn

By Sukh Sandhu

APRA's Prudential Standard CPS 230 Operational Risk Management has applied since 1 July 2025, and its transition period for existing service provider contracts ended on 1 July 2026. It is written for banks, insurers and superannuation trustees, but its core questions apply to any organisation that people depend on. This article explains the standard's main requirements and turns them into a practical checklist for regulated and unregulated organisations alike.

From preventing failure to surviving it

Traditional risk management asks how to stop bad things happening. Operational resilience starts from a different assumption: some disruptions will happen regardless, so the organisation must be able to keep delivering what matters most and recover quickly. The shift is from probability to consequence.

Recent events have made the point vividly. On 19 July 2024, a faulty software update from cyber security company CrowdStrike caused widespread failures of Windows computers worldwide. Microsoft estimated that about 8.5 million Windows devices were affected. Airlines, hospitals, banks, retailers and broadcasters were disrupted, including in Australia. Few of the affected organisations had done anything wrong themselves. Their exposure came from a dependency they did not control.

Regulators internationally have responded with operational resilience rules. In the United Kingdom, the Financial Conduct Authority and Prudential Regulation Authority required firms to identify important business services and set impact tolerances, with a deadline of 31 March 2025 to be able to remain within those tolerances. In the European Union, the Digital Operational Resilience Act has applied to financial entities since 17 January 2025. In Australia, the Australian Prudential Regulation Authority (APRA) produced CPS 230.

What CPS 230 is

CPS 230 was finalised by APRA in July 2023 and commenced on 1 July 2025. It replaced several older standards on outsourcing and business continuity management, including CPS 231 Outsourcing and CPS 232 Business Continuity Management and their superannuation equivalents, and brought operational risk, business continuity and service provider management together in one standard. APRA has also issued a supporting practice guide, CPG 230, which sets out guidance rather than requirements.

The standard applies to APRA-regulated entities: authorised deposit-taking institutions (ADIs), general insurers, life insurers, private health insurers and registrable superannuation entity (RSE) licensees.

Key principles

CPS 230 sets three overarching expectations. An APRA-regulated entity must:

- effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance
- maintain its critical operations within tolerance levels through severe disruptions
- manage the risks associated with the use of service providers

The standard defines operational risk broadly, as risks from inadequate or failed internal processes or systems, the actions or inactions of people, or external drivers and events. It requires entities to manage the full range of operational risks, expressly including legal, regulatory, compliance, conduct, technology, data and change management risk.

Key dates

Date	Event
July 2023	APRA releases final CPS 230
1 July 2025	CPS 230 commences
1 July 2025 to 30 June 2026	Pre-existing service provider contracts transition (earlier renewal applies)
1 July 2026	Deferred business continuity requirements apply to non-significant financial institutions
1 July 2026	Targeted amendments for certain non-traditional service providers take effect

Two transitional arrangements are important. First, where an entity had pre-existing contracts with service providers, the standard's requirements apply to those arrangements from the earlier of the next contract renewal date or 1 July 2026. Second, for non-significant financial institutions, certain business continuity requirements, covering the content of the business continuity plan, testing, annual updates and internal audit review, were deferred until 1 July 2026, with the old business continuity standards continuing to apply to them until 30 June 2026. At November 2026, both transitions have ended, and CPS 230 applies in full.

The 2026 amendments

On 30 April 2026, APRA finalised targeted amendments to CPS 230, taking effect on 1 July 2026. They give limited exemptions from specific contractual requirements for material arrangements with certain categories of non-traditional service providers, such as central banks and clearing and settlement facilities, which typically will not agree to standard contractual terms. The categories of exempt providers are listed in an attachment to the standard. APRA has described the exemptions as limited, and has said that the standard's other operational risk obligations are unaffected. APRA also updated CPG 230 and its register template to accommodate these arrangements.

The five pillars of CPS 230

1. Governance and accountability

The board is ultimately accountable for oversight of operational risk management. Among other things, CPS 230 requires the board to approve the business continuity plan and tolerance levels for disruptions to critical operations, review the results of testing and oversee the execution of findings. It must approve the service provider management policy and review risk and performance reporting on material service providers.

Senior management must provide clear and comprehensive information to the board on the expected impacts on critical operations when the board is making decisions that could affect their resilience. Senior management is responsible for operational risk management across the end-to-end process for all business operations. The board must also ensure that clear roles and responsibilities are set for senior managers, including for business continuity and service provider management.

2. Operational risk management

Entities must maintain internal controls designed and operating effectively for operational risks, with an assessment of their operational risk profile and a defined risk appetite supported by indicators, limits and tolerance levels. Incidents and near misses must be identified, escalated, recorded and addressed in a timely way, and taken into account in assessing the risk profile and control effectiveness.

APRA must be notified as soon as possible, and not later than 72 hours, after the entity becomes aware of an operational risk incident that it determines is likely to have a material financial impact or a material impact on its ability to maintain critical operations.

3. Critical operations and tolerance levels

This is the heart of the standard. Critical operations are processes undertaken by the entity or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on depositors, policyholders, beneficiaries or other customers, or on the entity's role in the financial system.

CPS 230 sets minimum lists. Unless it can justify otherwise, an entity must classify the following as critical operations:

Entity type	Minimum critical operations
ADI	Payments, deposit-taking and management, custody, settlements and clearing
Insurer (general, life, private health)	Claims processing
RSE licensee	Investment management and fund administration
All entities	Customer enquiries, and the systems and infrastructure supporting critical operations

For each critical operation, the entity must establish tolerance levels for three things:

1. the maximum period of time it would tolerate a disruption
2. the maximum extent of data loss it would accept as a result of a disruption

3. the minimum service levels it would maintain while operating under alternative arrangements

APRA can require an entity to review and change its tolerance levels and can set tolerance levels where it identifies heightened risk or material weakness. If a critical operation is disrupted outside tolerance, the entity must notify APRA as soon as possible and not later than 24 hours afterwards.

4. Business continuity

Entities must maintain a credible business continuity plan (BCP) that sets out how they would maintain critical operations within tolerance levels through disruptions, including disaster recovery planning for critical information assets. The BCP must include the register of critical operations and tolerance levels, triggers for activation, the actions the entity would take, an assessment of execution risks and dependencies, and a communications strategy.

The testing requirements are demanding. The entity must have a systematic testing program covering all critical operations, including an annual business continuity exercise. Testing must use a range of severe but plausible scenarios, including disruption to material service providers and scenarios where contingency arrangements are required. The BCP must be updated as needed on an annual basis, and the internal audit function must periodically review it and provide assurance to the board that the plan is credible and that testing is adequate.

5. Service provider management

Entities must maintain a comprehensive service provider management policy and a register of material service providers, which must be submitted to APRA annually. Material service providers are those the entity relies on to undertake a critical operation or that expose it to material operational risk. They may be third parties, related parties or connected entities.

Again there are minimum lists. For all APRA-regulated entities, providers of risk management, core technology services and internal audit must be classified as material unless the entity can justify otherwise. Sector-specific additions include credit assessment, funding and liquidity management and mortgage brokerage for ADIs, and underwriting, claims management, insurance brokerage and reinsurance for insurers.

The policy must also address fourth parties: the providers that a material service provider relies on to deliver a critical operation. Before entering into or materially changing a material arrangement, an entity must carry out due diligence and assess financial and non-financial risks, including concentration and geographic risks. Formal agreements must cover service levels, data ownership and control, audit access, sub-contracting, liability, force majeure and termination rights, and must allow APRA access to documentation and the right to conduct on-site visits.

APRA must be notified within 20 business days after entering into or materially changing an agreement for a service the entity relies on for a critical operation, and before entering into any material offshoring arrangement. The internal audit function must review any proposed material arrangement involving outsourcing of a critical operation and report

regularly to the board or audit committee on whether such arrangements comply with the service provider management policy.

Common implementation challenges

Industry commentary and APRA's own consultation process point to several areas where entities have found CPS 230 hard to implement.

- **Mapping end to end.** Identifying all the people, processes, technology, data, facilities and suppliers behind a critical operation takes far longer than expected, particularly where systems are old or ownership is fragmented.
- **Setting meaningful tolerances.** A tolerance of "24 hours" means little unless it has been tested against a realistic scenario and linked to customer harm.
- **Fourth parties.** Many entities have limited visibility of the subcontractors their providers rely on, especially in cloud services.
- **Contract remediation.** Bringing legacy contracts into line with the standard required renegotiation with providers who were not always willing to agree.
- **Testing realism.** Desktop exercises are easier than live failover tests, but the standard calls for severe but plausible scenarios that genuinely test the ability to stay within tolerance.

What non-APRA organisations can learn

CPS 230 does not apply to most Australian organisations. But its logic applies to any organisation whose customers, clients, patients, students, members or communities depend on it. Universities, hospitals, aged care providers, utilities, logistics companies, retailers, professional service firms and government agencies all have operations whose disruption would cause serious harm.

Some sectors already have related obligations. For example, responsible entities for certain critical infrastructure assets have risk management program obligations under the *Security of Critical Infrastructure Act 2018*. But for most organisations, operational resilience remains a matter of good governance rather than regulation.

In our view, five lessons translate directly.

Lesson 1: Identify what really matters

Ask which services, if disrupted, would cause genuine harm to the people who depend on you. For most organisations there are only a handful. A disability service provider might choose client care delivery and medication management. A professional services firm might choose client advice delivery, payroll and secure document handling. An education provider might choose teaching delivery, student records and fee processing.

Lesson 2: Set tolerances before the disruption

Decide in advance how long each service can be unavailable, how much data loss is acceptable and what minimum service you would maintain. The decision is the board's. It forces a frank conversation about whether current systems and suppliers can actually meet those expectations.

Lesson 3: Know your dependencies, including your suppliers' suppliers

The CrowdStrike outage showed that a single dependency can affect thousands of organisations simultaneously. Map the suppliers behind each important service, and ask your main technology providers who they rely on.

Lesson 4: Test against severe but plausible scenarios

Annual exercises that assume the building is unavailable for a day are not enough. Test scenarios such as a ransomware attack that encrypts core systems, the failure of a payroll or cloud provider, or a regional outage of telecommunications. Involve executives, not just the technology team.

Lesson 5: Get independent assurance

CPS 230 requires internal audit to review the business continuity plan and outsourcing of critical operations. For any organisation, independent review of resilience arrangements, whether by internal audit or an external reviewer, helps the board avoid relying solely on management's confidence. This also aligns with the IIA's Organizational Resilience Topical Requirement, which the IIA lists as effective from 30 April 2027.

> *Resilience is not the absence of disruption. It is the ability to keep delivering what matters while disruption happens.*

Questions directors should ask

Whether or not CPS 230 applies, directors can test their organisation's resilience with a handful of direct questions at the next board or committee meeting.

1. Which of our operations would cause serious harm to people who depend on us if they stopped for a day, a week or a month?
2. Has the board approved a maximum tolerable disruption, acceptable data loss and minimum service level for each of them?
3. When did we last test our ability to stay within those limits, using a scenario that genuinely stretched us, and what did we learn?
4. Which suppliers could stop those operations, and what is our plan if one of them fails without warning?
5. Do we know which subcontractors our most important technology providers depend on?
6. Who provides independent assurance that our continuity plans are credible, and when did the board last see their findings?
7. If a serious disruption happened tonight, who would decide to activate the plan, and how would we communicate with customers, staff and regulators?

Clear answers to these questions are a good sign. Vague answers, or answers that depend on one or two individuals, suggest the organisation's resilience has not yet been tested in a way the board can rely on.

An operational resilience checklist

This checklist draws on the structure of CPS 230. APRA-regulated entities must meet the standard itself; other organisations can use it as a practical guide.

Governance

- Board has approved which services or operations are critical
- Board has approved tolerance levels for each critical operation
- Board receives regular reporting on resilience, testing results and material suppliers
- A named executive is accountable for each critical operation end to end

Critical operations and tolerances

- Register of critical operations with a short rationale for each
- Tolerances for maximum disruption time, maximum data loss and minimum service levels
- Tolerances linked to the harm that would be caused to customers or stakeholders
- End to end maps of people, processes, technology, data, facilities and suppliers for each critical operation

Business continuity

- Business continuity plan covering all critical operations, with activation triggers and clear roles
- Disaster recovery plans for critical information assets
- Communications strategy for staff, customers, regulators and the media
- Annual exercise using severe but plausible scenarios, including supplier failure
- Plan updated at least annually and after significant changes or incidents

Service providers

- Register of material service providers, including related parties
- Due diligence before engaging or materially changing a material provider
- Contracts covering service levels, data, audit rights, subcontracting, termination and exit
- Visibility of key fourth parties
- Tested exit or substitution plans for the most critical providers

Incidents and assurance

- Incident and near miss process that feeds back into risk and control assessments
- Notification obligations understood and documented (for APRA-regulated entities: 72 hours for material operational risk incidents, 24 hours for disruptions outside tolerance, 20 business days for new or materially changed critical arrangements)
- Internal audit or independent review of continuity plans and critical outsourcing

What to do this month

1. Ask the executive team to list no more than ten operations whose disruption would cause serious harm, and bring the list to the board.

2. For the top three, write down current tolerances for disruption time, data loss and minimum service, even if they are only estimates.
3. Identify the five suppliers whose failure would most disrupt those operations and check what your contracts say about continuity, data and exit.
4. Schedule a severe but plausible exercise for the executive team in the next six months.
5. Ask internal audit, or an independent reviewer, to include resilience in next year's plan.
6. For APRA-regulated entities, confirm that all legacy contracts have now been brought into line with the standard, since the transition period ended on 1 July 2026, and check whether any arrangements rely on the 2026 exemptions for non-traditional service providers.

The bottom line

CPS 230 is the most significant change to operational risk regulation in Australian financial services in many years. Its central idea is simple: decide what must keep running, decide how much disruption you can bear, know who you depend on, and prove through testing that you can stay within your limits. In our view, organisations outside APRA's reach would be wise to borrow that discipline before a disruption forces the lesson on them.

Sources

- Australian Prudential Regulation Authority, Prudential Standard CPS 230 Operational Risk Management (compiled version, July 2025), https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20clean.pdf
- Australian Prudential Regulation Authority, Operational risk management consultation and final standard, https://www.apra.gov.au/consultations/operational-risk-management
- Australian Prudential Regulation Authority, APRA finalises targeted amendments to CPS 230 Operational Risk Management, 30 April 2026, https://www.apra.gov.au/news-and-publications/apra-finalises-targeted-amendments-cps-230-operational-risk-management
- Australian Prudential Regulation Authority, APRA to consult on targeted changes to CPS 230 for non-traditional service providers, 31 October 2025, https://www.apra.gov.au/news-and-publications/apra-consult-targeted-changes-cps-230-non-traditional-service-providers
- Clayton Utz, CPS 230: prepare for APRA's incoming operational risk management standard by refreshing outsourcing processes and contracts, March 2025, https://claytonutz.com/insights/2025/march/cps230-prepare-for-apras-incoming-operational-risk-management-standard-by-refreshing-outsourcing-processes-and-contracts
- Corrs Chambers Westgarth, APRA's new CPS 230: key requirements for regulated entities and their service providers, https://www.corrs.com.au/insights/apras-new-cps-230-key-requirements-for-regulated-entities-and-their-service-providers

- Microsoft, Helping our customers through the CrowdStrike outage, 20 July 2024, https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/
- Financial Conduct Authority, PS21/3 Building operational resilience, March 2021, https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience
- European Insurance and Occupational Pensions Authority, Digital Operational Resilience Act (DORA), https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
- Cyber and Infrastructure Security Centre, Security of Critical Infrastructure Act 2018 obligations, https://www.cisc.gov.au/
- The Institute of Internal Auditors, Issued and upcoming Topical Requirements, accessed November 2026, https://www.theiia.org/en/standards/2024-standards/topical-requirements/

PART 3

Risks on the board agenda

Fraud, mandatory climate reporting and assurance, and cyber risk.

ON THE BOARD AGENDA

Fraud, What the Data Shows: Lessons From 2,402 Cases and the Australian Standard

By Sukh Sandhu

The world's largest study of occupational fraud has a blunt message for boards and managers: most frauds are found because someone speaks up, and most succeed because a control was missing or overridden. Read alongside Australian Standard AS 8001:2021 and the new corporate offence of failing to prevent foreign bribery, the evidence points to a practical fraud control agenda that any organisation can start this month.

The study and why it matters

Every two years the Association of Certified Fraud Examiners (ACFE) publishes its Report to the Nations, a survey of Certified Fraud Examiners about real cases they investigated. The latest edition at November 2026 is *Occupational Fraud 2026: A Report to the Nations*, the 14th edition of the study. It analyses 2,402 cases of occupational fraud investigated between January 2024 and September 2025, drawn from 143 countries and territories. The cases caused total losses of more than US$3.4 billion.

Occupational fraud, in the ACFE's sense, is fraud committed by people against the organisations that employ them: an employee, manager, owner or executive using their position to enrich themselves by misusing the organisation's resources or assets. It is not the same as external scams or cybercrime, although the lines increasingly blur when an insider helps an outsider, or when a payment redirection scam succeeds because nobody checked a change of bank details.

Two caveats are worth keeping in mind. First, the data comes from cases that were detected and investigated by fraud examiners, so it says nothing directly about frauds that are never found. Second, the figures are reported in US dollars and are global. Australia contributed 25 cases to the Asia-Pacific sample. The report is best read as a picture of patterns, not a precise forecast for any one organisation.

The headline numbers

The 2026 key findings are summarised below. All dollar figures are US dollars.

Measure	2026 finding
Cases analysed	2,402 from 143 countries and territories
Total losses	More than $3.4 billion
Median loss per case	$104,000

Measure	2026 finding
Average loss per case	$1,457,000
Typical duration before detection	12 months
Estimated share of revenue lost	5% each year (CFE estimate)
Detected by tip	43% of cases

The median loss of US$104,000 is lower than the 2024 edition's US$145,000, and the ACFE notes that losses have resumed a downward trend while the median duration has stayed level. The gap between the median and the average is the important feature: a small number of very large frauds pull the average to almost US$1.5 million. In practical terms, most frauds are medium sized and slow, and a few are catastrophic.

The 5% of revenue figure deserves care. It is an estimate given by the surveyed fraud examiners, not a measured loss rate. It is useful as a conversation starter in a boardroom, but it should not be dropped into a budget as if it were an audited number.

The three scheme types

The ACFE classifies occupational fraud into three families.

- **Asset misappropriation** was present in 90% of cases, with a median loss of US$100,000. These are the most common and least costly schemes: billing schemes, theft of noncash assets, expense reimbursement fraud, payroll fraud and cheque and payment tampering.
- **Corruption** featured in 45% of cases, with a median loss of US$150,000. Corruption includes bribery, kickbacks, conflicts of interest and economic extortion.
- **Financial statement fraud** occurred in 6% of cases but had a median loss of US$1,000,000. It is rare and extremely damaging.

In the Asia-Pacific region, which includes Australia, corruption was even more prominent. The report records corruption in 61% of the 143 Asia-Pacific cases, with a regional median loss of US$150,000. That matters for Australian organisations that trade or source across the region, and it is one reason the new foreign bribery offence, discussed below, deserves board attention.

How fraud is found

The detection data is the most useful part of the report for anyone designing controls.

Initial detection method	Share of cases
Tip	43%
Internal audit	15%
Management review	13%
Document examination	5%
Account reconciliation	5%
By accident	4%
Automated transaction or data monitoring	3%
External audit	2%

Tips were the leading method by a wide margin, uncovering nearly three times as many cases as the next most common method. Of those tips, 55% came from employees, 21%

from customers, 14% were anonymous and 11% came from vendors. Web based reporting (46%) and email (34%) both surpassed telephone hotlines (23%) as the most common channels used by whistleblowers.

Two lessons follow. The first is that a reporting channel is not a box to tick: it is the single most productive fraud detection tool most organisations have. The second is that channels must match how people actually communicate. A phone number on a poster in the lunch room is no longer enough.

The low figure for external audit, 2%, is not a criticism of auditors. A financial statement audit is designed to obtain reasonable assurance that the financial report is free of material misstatement. It is not designed to find every theft, and boards that rely on the external audit as their fraud detection strategy are relying on something that was never built for that purpose.

Active detection beats passive detection

The ACFE separates detection methods into passive methods, where the fraud surfaces without effort by the organisation (notification by police, accident, confession), and active methods, such as account reconciliation, document examination and surveillance and monitoring. The 2026 report finds that frauds uncovered by proactive methods produced lower losses and were found sooner, and suggests fraud can be uncovered up to four times faster with active methods. Frauds first identified through notification by law enforcement had a median duration of 24 months and a median loss of US$890,000.

Who commits fraud, and the warning signs

Fraud by owners and executives is less frequent than fraud by staff but far more costly. The 2026 study found median losses of US$475,000 for owner and executive frauds against US$50,000 for frauds by employees, more than nine times greater. Frauds involving three or more perpetrators caused a median loss of US$324,000, almost six times the US$55,000 median for a single perpetrator. Collusion defeats segregation of duties, which is why it is so expensive. The study also found that the longer a fraudster had worked for the organisation, the more costly the fraud tended to be.

More than half of all cases came from five departments: operations (13%), accounting (13%), sales (10%), customer service (10%) and executive or upper management (10%).

Behavioural red flags

In 84% of cases the perpetrator displayed at least one behavioural red flag, and more than half of cases involved multiple flags. The most common, as in every edition of the study, was living beyond one's means, observed in 39% of cases, followed by financial difficulties. Other recognised flags include:

- an unusually close association with a vendor or customer;
- control issues and unwillingness to share duties;
- refusal to take leave;
- irritability, suspiciousness or defensiveness;
- bullying or intimidation;

- a "wheeler dealer" attitude;
- past legal problems or employment problems.

Two cautions apply. Red flags are indicators, not evidence, and 16% of frauds occurred with no red flag observed at all. And in our view, the purpose of red flag awareness is to prompt a proportionate look at transactions and access, not to justify surveillance of people's private lives or assumptions about anyone experiencing personal hardship. A good fraud program combines behavioural awareness with transaction data, so that suspicion is tested against evidence quickly and fairly.

Transactional red flags

Behaviour is only half the picture. Common transactional warning signs in Australian organisations include:

- new vendors with no clear business purpose, or vendors sharing a bank account, address or phone number with an employee;
- requests to change a supplier's bank details by email;
- invoices just below an approval threshold, or split purchases;
- round dollar or sequential invoice numbers from the same supplier;
- journal entries posted late, by senior staff, to unusual accounts;
- expense claims without receipts, duplicated across periods, or at weekends;
- payroll records for people with no leave history, no tax file changes and no manager.

Why controls fail

The ACFE asks examiners to name the primary internal control weakness that allowed each fraud.

Primary control weakness	Share of cases
Lack of internal controls	33%
Override of existing internal controls	19%
Lack of management review	18%
Poor tone at the top	7%
Lack of competent personnel in oversight roles	7%
Lack of independent checks or audits	4%

The first three weaknesses together accounted for 70% of all frauds. When a lack of internal controls was the primary factor, median losses were 43% higher than the overall median. For frauds by owners and executives, poor tone at the top was the third most common factor.

The controls that make a difference

The report examined 18 anti-fraud controls and found that all 18 were associated with lower median losses and faster detection. On average, the presence of a control reduced losses by 37% compared with organisations without that control. Four controls stood out for the largest reductions in both loss and duration: management review, proactive data monitoring and analysis, a code of conduct, and surprise audits.

Control	Lower losses	Faster detection

Control	Lower losses	Faster detection
Surprise audits	50%	50%
Management review	55%	44%
Proactive data monitoring and analysis	53%	44%

Surprise audits are notable because they are among the least used controls. In the Asia-Pacific region, only 34% of victim organisations used them, compared with 87% that had a code of conduct. Job rotation or mandatory leave was in place at just 18% of Asia-Pacific victims.

A further finding should concern every board. Eighty per cent of victim organisations modified their anti-fraud controls after the fraud. In our view, many of those changes could have been made before the loss, at a fraction of the cost.

The Australian benchmark: AS 8001:2021

In Australia, the reference point for fraud control is AS 8001:2021 *Fraud and Corruption Control*, published by Standards Australia on 11 June 2021. It is the third edition and superseded AS 8001:2008. It applies to organisations of all types and sizes, including for profit, not for profit and public sector entities.

Compliance with the standard is voluntary unless a law, contract or policy makes it mandatory. Some public sector bodies, regulators and funding agreements reference it, and it is widely used as the benchmark when auditors, insurers and investigators assess whether an organisation's fraud program was reasonable.

What changed in 2021

The 2021 edition made several changes that matter for boards and managers.

- **A system, not a plan.** The earlier emphasis on a fraud control plan was replaced by a fraud and corruption control system (FCCS): the documented framework of policies, processes, roles and controls through which an organisation manages fraud and corruption risk.
- **Clear governing body and top management roles.** The standard sets out what the governing body and top management are expected to do, including oversight, resourcing and setting the tone.
- **Broader scope.** The standard addresses fraud against the organisation and fraud by the organisation, and it gives attention to technology enabled fraud.
- **Alignment with other standards.** It was harmonised with the anti-bribery management systems standard, AS ISO 37001, and sits alongside standards on whistleblowing management (ISO 37002) and compliance management (ISO 37301).

The standard is broadly organised around the foundations of a control system (governance, culture, roles, risk assessment), followed by prevention, detection and response. That structure maps neatly onto the ACFE evidence: prevention is where codes of conduct, segregation and vendor controls sit; detection is where reporting channels, reconciliations and data analytics sit; and response covers investigation, recovery, discipline, referral to police and fixing the control gap.

The ACFE data tells you which controls work. AS 8001:2021 tells you how to organise them into a system that someone owns.

Context: the failure to prevent foreign bribery offence

From 8 September 2024, a new corporate offence in section 70.5A of the Criminal Code applies to companies that fail to prevent foreign bribery by their associates. It was introduced by the *Crimes Legislation Amendment (Combatting Foreign Bribery) Act 2024*.

The key features are as follows.

- **Who is caught.** A company commits the offence if an associate bribes a foreign public official for the company's profit or gain. Associates include officers, employees, agents and contractors, subsidiaries, and others who perform services for or on behalf of the company.
- **Absolute liability.** The company can be liable even if it did not know about the bribe and did not intend it.
- **One defence.** The only defence is that the company had adequate procedures designed to prevent its associates from committing foreign bribery.
- **Penalties.** The maximum penalty for a company is the greatest of 100,000 penalty units, three times the benefit obtained from the bribe, or, where that benefit cannot be determined, 10% of annual turnover.

The same Act broadened the existing foreign bribery offence, replacing the "not legitimately due" test with an improper influence test and extending the offence to bribes for a personal advantage, not only a business advantage.

The Attorney-General's Department published guidance on adequate procedures in August 2024. It sets out six principles: fostering a control environment, responsibilities of top level management, risk assessment, communication and training, reporting foreign bribery, and monitoring and review. The guidance emphasises that procedures should be proportionate to the company's risk profile.

Why does this belong in an article about fraud? Because the controls overlap almost entirely. Third party due diligence, gifts and hospitality registers, payment approvals, agent and intermediary contracts, and a trusted reporting channel all serve both purposes. An organisation that has built a credible fraud and corruption control system against AS 8001:2021 is well placed to show adequate procedures. One that has not will struggle on both fronts. The guidance is not legal advice for any particular company, and directors with overseas operations, agents or government customers should take specific legal advice.

A fraud control checklist

The checklist below draws together the ACFE evidence, the structure of AS 8001:2021 and the adequate procedures guidance. It is a starting point, not a certification.

Governance and culture

1. The board or audit and risk committee has formally assigned oversight of fraud and corruption risk and receives a report on it at least twice a year.
2. A senior executive owns the fraud and corruption control system and has the resources and authority to run it.
3. A code of conduct covers fraud, bribery, conflicts of interest, gifts and hospitality, and is acknowledged by staff, directors and key contractors.
4. Executives model the standard, including disclosing their own conflicts and complying with the same approval rules as everyone else.

Risk assessment

1. A documented fraud and corruption risk assessment covers each business unit, including procurement, payroll, payments, sales incentives, inventory, financial reporting and technology enabled fraud.
2. The assessment considers management override and collusion, not just individual staff fraud.
3. Foreign bribery risk is assessed for any overseas operations, agents, intermediaries, joint ventures or government touchpoints.
4. The assessment is refreshed at least annually and after any significant change, incident or acquisition.

Prevention

1. Segregation of duties is in place for creating vendors, approving invoices and releasing payments, with compensating review where staff numbers are small.
2. Changes to supplier bank details are verified by phone using contact details already on file, never from the request itself.
3. Pre-employment screening is proportionate to the role, and screening of third parties and agents is risk based.
4. Delegations of authority are documented, enforced in systems, and reviewed for split transactions.
5. Mandatory leave or job rotation applies to roles with sole control over cash, payments or inventory.

Detection

1. A reporting channel offers web, email and phone options, allows anonymous reports, and is promoted to staff, customers and suppliers.
2. Whistleblower protection arrangements meet the Corporations Act requirements where they apply.
3. Management review of accounts and exception reports is scheduled, evidenced and followed up.
4. Proactive data analytics runs regularly over payments, vendor master files, payroll, expenses and journals.
5. Surprise audits or unannounced counts are part of the internal audit plan.

Response

1. An investigation protocol sets out who investigates, how evidence is preserved, when to involve lawyers and police, and how the board is informed.
2. Recovery options, including insurance notification, are considered early.
3. Every confirmed fraud ends with a root cause review and a documented control fix.

What to do this month

1. **Test your channel.** Make a test report through each channel and time how long it takes to reach someone who can act. Check that suppliers and customers can find it.
2. **Run three analytics.** Match the vendor master file to the employee master file on bank account, address and phone; list all supplier bank detail changes in the past 12 months and confirm each was verified; and list invoices within 5% below each approval limit.
3. **Schedule one surprise audit.** Choose a high risk area, such as petty cash, inventory, fuel cards or corporate credit cards, and do not announce the date.
4. **Map the control weaknesses.** Ask your internal auditor or finance lead which key controls are missing, which can be overridden by a single senior person, and where management review is not evidenced.
5. **Check your third parties.** If you use agents or intermediaries overseas or deal with foreign officials, confirm due diligence, contract clauses and payment approvals are in place, and compare your program with the Attorney-General's Department guidance.
6. **Put fraud on the next committee agenda.** Bring the ACFE detection and control tables to the audit and risk committee and ask management to benchmark your program against them and against AS 8001:2021.

The bottom line

The data has been consistent for years and the 2026 edition confirms it. Fraud is usually found by people, not systems. It usually happens where a control was missing or a senior person could override it. And it costs less when organisations look actively instead of waiting to be told. In our view, the organisations that do best are not those with the longest policy manuals, but those where staff know how to raise a concern, managers actually review what they sign, and someone checks the data before the loss becomes a headline.

Sources

- Association of Certified Fraud Examiners, *Occupational Fraud 2026: A Report to the Nations*, 2026, https://www.acfe.com/report-to-the-nations.aspx
- Association of Certified Fraud Examiners, Press releases (including 2024 and 2026 Report to the Nations releases), https://www.acfe.com/press-release.aspx?id=4740
- Standards Australia, AS 8001:2021 Fraud and Corruption Control, 11 June 2021, https://store.standards.org.au/product/as-8001-2021
- McGrathNicol, Standards Australia releases AS 8001:2021 Fraud and Corruption Control, 2021, https://www.mcgrathnicol.com/insight/standards-australia-releases-as-8001-2021-fraud-and-corruption-control/

- BDO Australia, AS8001: Are you ready for the changes to fraud and corruption control?, 2021, https://www.bdo.com.au/en-au/insights/forensic-services/articles/as8001-are-you-ready-for-the-changes-to-fraud-and-corruption-control
- Attorney-General's Department, Guidance on adequate procedures to prevent the commission of foreign bribery, August 2024, https://consultations.ag.gov.au/crime/draft-guidance-on-adequate-procedures/user_uploads/guidance-on-adequate-procedures-to-prevent-the-commission-of-foreign-bribery.pdf
- A&O Shearman, Combatting foreign bribery: a closer look at Australia's new legislation, 2024, https://www.aoshearman.com/en/insights/combatting-foreign-bribery-a-closer-look-at-australias-new-legislation
- Ashurst, Are your company's anti-bribery controls fit for purpose?, 2024, https://ashurst.com/en/insights/are-your-companys-anti-bribery-controls-fit-for-purpose

ON THE BOARD AGENDA

Climate Reporting and Assurance in Australia: What the Law Requires and What Comes Next

By Sukh Sandhu

Australia's mandatory climate reporting regime is no longer a future project. The first cohort of large entities has lodged audited sustainability reports, ASIC has published its first review of them, and the second cohort's first reporting year is already under way. This article sets out the law, the standards, the assurance timetable and the practical steps directors and auditors should be taking at November 2026.

How we got here

The legal foundation is Schedule 4 of the *Treasury Laws Amendment (Financial Market Infrastructure and Other Measures) Act 2024*, which received Royal Assent on 17 September 2024. It amended the *Corporations Act 2001* so that entities required to prepare an annual financial report under Chapter 2M, and that meet the sustainability reporting thresholds in section 292A, must also prepare an annual sustainability report.

At present, the sustainability report covers climate only. It consists of:

- the climate statements required by the sustainability standards;
- any notes to those statements;
- any statements and notes on other environmental sustainability matters that the Minister may later require by legislative instrument; and
- the directors' declaration about the statements and notes.

The report is lodged with the financial report, the directors' report and the auditor's reports. In effect, climate disclosure has moved from the glossy voluntary report into the statutory annual report, with the same lodgement, director sign off and audit architecture as the financial statements.

The standards: AASB S2 and AASB S1

The Australian Accounting Standards Board (AASB) issued two Australian Sustainability Reporting Standards on 20 September 2024, both operative for reporting periods beginning on or after 1 January 2025.

- **AASB S2 Climate-related Disclosures** is the mandatory standard. It is based on the International Sustainability Standards Board's IFRS S2 and incorporates the general requirements needed to make it work on its own for climate disclosures.

- **AASB S1 General Requirements for Disclosure of Sustainability-related Financial Information** is voluntary. The AASB issued it as a voluntary standard because Government policy is to mandate only climate-related financial disclosures at present. Apart from being voluntary, it closely follows IFRS S1.

AASB S2 requires disclosures in four areas familiar to anyone who has followed the Task Force on Climate-related Financial Disclosures:

Pillar	What must be disclosed
Governance	The bodies and individuals that oversee climate risks and opportunities, and management's role
Strategy	Climate risks and opportunities, their current and anticipated financial effects, transition plans, and climate resilience using scenario analysis
Risk management	How climate risks and opportunities are identified, assessed, prioritised and monitored
Metrics and targets	Scope 1, Scope 2 and Scope 3 greenhouse gas emissions, cross industry metrics, and any climate targets

AASB S2 contains transitional reliefs. In particular, an entity does not have to disclose Scope 3 emissions in its first annual reporting period under the standard, and comparative information is not required in the first year.

Who reports, and when

The Corporations Act phases entities in by size, using three groups. A company is in a group if it meets at least two of the three size tests for that group, or meets one of the emissions or asset owner tests.

Group	First financial years starting on or after	Size tests (two of three)	Other entry routes
Group 1	1 January 2025	Revenue $500m or more; gross assets $1b or more; 500 or more employees	Registered under the NGER Act and above the publication threshold
Group 2	1 July 2026	Revenue $200m or more; gross assets $500m or more; 250 or more employees	Any NGER registered corporation; asset owners with $5b or more in assets
Group 3	1 July 2027	Revenue $50m or more; gross assets $25m or more; 100 or more employees	None

Group 3 entities that have no material climate risks or opportunities can make a statement to that effect instead of full climate disclosures, although they must explain how they reached that conclusion.

A proposed change for smaller entities

In the 2026 to 27 Budget, the Government announced it would consult on raising the large proprietary company thresholds in section 45A of the Corporations Act, lifting the revenue test from $50 million to $100 million and the assets test from $25 million to $50

million. ASIC has noted that, if adopted, some entities expecting to report as Group 3 entities may no longer need to prepare a financial report or a sustainability report. At November 2026 these changes are not in effect, and ASIC states that the existing thresholds continue to apply. Entities near the line should plan on the current law while watching for legislation.

Assurance: the ASSA 5010 timetable

Sustainability reports must be audited or reviewed by the entity's auditor. The detail is set by the Auditing and Assurance Standards Board (AUASB) in ASSA 5010 *Timeline for Audits and Reviews of Information in Sustainability Reports under the Corporations Act 2001*, made on 28 January 2025 and amended by ASSA 2025-10 on 17 December 2025. In ASSA 5010, a review means a limited assurance engagement and an audit means a reasonable assurance engagement.

The amended standard sets a simple progression for each group.

Reporting year	Assurance required
First year	Limited assurance over governance, strategy (risks and opportunities), Scope 1 and Scope 2 emissions, and any statement that there are no material climate risks or opportunities
Second and third years	Limited assurance over all disclosures in the sustainability report
Fourth year onwards	Reasonable assurance over all disclosures

Mapped to calendar dates, the fourth year of reporting begins with financial years commencing on or after 1 July 2028 for Group 1, 1 July 2029 for Group 2, and 1 July 2030 for Group 3. The Corporations Act itself requires reasonable assurance of all mandatory climate disclosures for financial years commencing on or after 1 July 2030.

Two practical points are often missed. Group 1 entities with years beginning 1 January are subject to the first year provisions twice (for years commencing 1 January 2025 and 1 January 2026). And comparatives that were not assured, or were only subject to limited assurance, in the prior year do not need to be brought up to the current year's assurance level.

> *Year one assurance is narrow. Year two is broad. Year four is an audit. Systems built only to survive year one will not survive year four.*

The difference between limited and reasonable assurance is not cosmetic. Limited assurance provides a negative form of conclusion based mainly on inquiry and analytical procedures. Reasonable assurance requires the auditor to gather sufficient appropriate evidence to express a positive opinion, which in turn requires the entity to have documented processes, internal controls and data trails over emissions, scenario analysis and financial effects that are robust enough to be tested.

Liability: the modified regime

Climate disclosures involve estimates, assumptions and forward looking judgements. To give preparers time to develop methods, the Act includes a temporary modified liability regime in section 1707D of the Corporations Act.

For a limited period, statements about Scope 3 emissions, scenario analysis and transition plans in a sustainability report are protected statements. During that period, legal actions in relation to those statements are limited to proceedings brought by ASIC and criminal proceedings. Private litigants cannot sue over them. The protection applies to financial years commencing in the three year window from 1 January 2025. For financial years commencing in 2025, protection also extends to forward looking climate statements required by the sustainability standards.

This protection is narrow and temporary. It applies only to statements made to comply with a sustainability standard. It does not protect voluntary statements made outside the sustainability report, such as in investor presentations, websites or promotional material, although a statement repeated in a document required by another Commonwealth law (such as a product disclosure statement) can be protected if it is the same as the protected statement. Outside the first year's forward looking statements, it does not cover governance, Scope 1 or Scope 2 disclosures. And it ends. In our view, boards should treat the modified liability period as time to build defensible processes, not as permission to publish loosely supported claims.

The directors' declaration

Directors must make a declaration about the sustainability report, as they do for the financial report. For financial years commencing in the first three years of the regime, the declaration is modified: directors state whether, in their opinion, the entity has taken reasonable steps to ensure the substantive provisions have been complied with. After that transition, the declaration becomes a direct statement of compliance. The step up in the declaration lines up closely with the move to reasonable assurance.

ASIC's approach: RG 280 and the first review

ASIC administers the regime. It released Regulatory Guide 280 *Sustainability reporting* (RG 280) on 31 March 2025, after consulting on a draft from 7 November 2024 and receiving 60 submissions. RG 280 explains who must prepare a sustainability report, what it must contain, how to treat sustainability information disclosed elsewhere, and how ASIC will administer the regime, including its approach to relief and its directions power. The final guide added sections on scenario analysis and Scope 3 emissions, and more specific guidance for directors.

ASIC has said it will take a pragmatic and proportionate approach to supervision and enforcement while the requirements are phased in. Where a statement appears incorrect or misleading, ASIC will generally engage with the entity first and may give it an opportunity to correct the statement or use its directions power. ASIC has also said it is more likely to commence an enforcement investigation where there is serious or reckless misconduct, or where a required report has not been prepared.

Report 839: the first look at mandatory reports

On 21 September 2026 ASIC published Report 839, its review of a sample of the first Group 1 sustainability reports, together with media release 26-222MR. ASIC reviewed 40 of the 312 sustainability reports lodged by Group 1 entities with 31 December 2025 year ends, split evenly between listed and unlisted entities.

ASIC found that statutory reporting has improved the quantity and quality of climate information compared with earlier voluntary disclosures, and that entities generally met the basic requirements to prepare, lodge and have their reports audited. It also observed mixed practice in forward looking disclosures and in areas that rely on judgement, particularly strategy and metrics and targets. ASIC's findings include these:

- 67.5% of reviewed entities identified the board as overseeing climate risks and opportunities;
- 42.5% incorporated climate factors into executive remuneration;
- 37.5% provided only qualitative information on the current and anticipated financial effects of climate risks and opportunities;
- 82.5% relied on the first year relief for Scope 3 emissions, which will not be available in their second reporting year;
- 47.5% disclosed climate transition plans.

ASIC did not direct any entity to amend its report in this first cycle. It set out eight practical actions for preparers, including explaining the connections between the sustainability report and the financial report, explaining why quantitative information is omitted, disclosing judgements and measurement uncertainty clearly, including legally required targets such as Safeguard Mechanism obligations, avoiding voluntary disclosures that obscure material information, and avoiding disclaimers that discourage reliance on the report. ASIC has said its next review, in 2026 to 27, will cover a sample of Group 1 reports for years ending 30 June 2026, and that it will continue to engage with the large audit firms on assurance methodologies.

What directors should do now

The obligations sit squarely with directors. The sustainability report is part of the statutory reporting package, directors make the declaration, and directors' duties of care and diligence apply to how they oversee it. The list below applies the law and ASIC's guidance to the boardroom.

For Group 1 boards

1. **Plan for Scope 3.** Most Group 1 entities used the first year relief. Confirm that management has a method, data sources and assurance plan for Scope 3 in the second year.
2. **Prepare for broader assurance.** From the second year, limited assurance covers every disclosure, including scenario analysis, transition plans and metrics. Ask the auditor where the first year engagement found weaknesses.
3. **Read Report 839 against your own report.** Ask management to map your report against ASIC's eight actions and identify gaps.

4. **Look at connectivity.** Check that assumptions used in the climate statements, such as carbon prices, asset lives and impairment drivers, are consistent with the financial report, or that differences are explained.

For Group 2 boards

1. **Your first year has started.** For a 30 June year end company, the first Group 2 financial year began on 1 July 2026. The first report and limited assurance over governance, strategy and Scope 1 and 2 emissions will follow.
2. **Agree the assurance plan early.** Meet the auditor now to agree scope, materiality, data access and timing, and consider a readiness review.
3. **Document governance.** Record which board committee oversees climate risk, how often it meets on the topic, and what competencies directors have or can access.

For Group 3 and those near the threshold

1. **Confirm your status.** Test the thresholds now on current law. If you may fall into Group 3, start the materiality assessment that determines whether you will make full disclosures or a statement of no material climate risks.
2. **Watch the reform.** Track the proposed change to the large proprietary company thresholds, but do not stop preparation in anticipation of it.

For all reporting entities

1. **Treat it like financial reporting.** Assign an accountable executive, build a control environment over climate data, and give the audit committee clear oversight.
2. **Align every channel.** Voluntary statements outside the sustainability report do not get modified liability protection. Make sure investor presentations, websites and offer documents are consistent with the report.
3. **Engage the value chain sensibly.** RG 280 includes guidance for value chain entities, including small businesses and farmers. Ask suppliers for what you actually need.

What auditors should do now

For audit firms and audit committees, the work is equally concrete.

- **Competence and independence.** Sustainability assurance requires climate and emissions expertise. Firms must make sure engagement teams and any experts used meet the requirements of the AUASB standards, and audit committees should ask how the firm has resourced the engagement.
- **Plan backwards from reasonable assurance.** The jump to an audit in the fourth year is significant. Auditors should identify now which controls and records will need to support a positive opinion, and say so to management.
- **Communicate findings.** First year review findings are the best early warning a board has. Auditors should report control deficiencies and data quality issues clearly to the audit committee.
- **Coordinate with the financial audit.** Because ASIC is focused on connectivity, the financial statement audit team and the sustainability assurance team should share their understanding of key climate assumptions.

A board checklist for the next sustainability report

Question	Owner
Are we in Group 1, 2 or 3 under current law, and when does our first year start?	Company secretary, CFO
Which committee oversees climate risk and the sustainability report?	Board chair
What assurance applies this year, and what will apply next year?	CFO, external auditor
Is Scope 3 planned, with methods and data sources agreed?	Sustainability lead
Are scenario analysis assumptions consistent with the financial report?	CFO
What did the auditor's last review find?	Audit committee chair
Are statements outside the report consistent with it?	General counsel
Have we read ASIC Report 839 and compared our report with its eight actions?	Management

What to do this month

1. Put the sustainability report on the next audit and risk committee agenda, with a status update on group classification, timeline and assurance scope.
2. Ask management for a short gap analysis against ASIC Report 839's eight actions.
3. Meet the external auditor to confirm the scope and timing of the next sustainability engagement, and ask what the step to reasonable assurance will require.
4. Confirm who owns Scope 3 data and what the plan is for the year in which first year relief no longer applies.
5. Review the investor presentation, website and annual report narrative for climate claims that are not supported by, or are inconsistent with, the sustainability report.
6. Diarise the consultation on threshold changes, and assign someone to track it.

The bottom line

Australia has chosen a model that puts climate disclosure inside the statutory annual report, signed off by directors and assured by the auditor, with a phased path from limited to reasonable assurance. The first year has shown that entities can meet the basic requirements. The harder years are ahead: Scope 3, scenario analysis and transition plans under broader assurance, followed by a full audit. In our view, the organisations that will cope best are those that build climate reporting into their finance function now, rather than treating it as a separate exercise each year.

Sources

- Federal Register of Legislation, Treasury Laws Amendment (Financial Market Infrastructure and Other Measures) Act 2024, assented 17 September 2024, https://www.legislation.gov.au/C2024A00087/asmade/text
- ASIC, Sustainability reporting (overview and proposed threshold changes), accessed November 2026, https://asic.gov.au/regulatory-resources/sustainability-reporting/

- ASIC, Regulatory Guide 280 Sustainability reporting, 31 March 2025, https://www.asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-280-sustainability-reporting
- ASIC, 25-051MR ASIC issues sustainability reporting regulatory guide, 31 March 2025, https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2025-releases/25-051mr-asic-issues-sustainability-reporting-regulatory-guide
- ASIC, Report 839, 21 September 2026, https://download.asic.gov.au/media/osle1xu2/rep839-published-21-september-2026.pdf
- ASIC, 26-222MR ASIC observes improved sustainability reporting and notes areas for further development, September 2026, https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-222mr-asic-observes-improved-sustainability-reporting-and-notes-areas-for-further-development/
- Ashurst, ASIC's first comprehensive review of sustainability reports, 7 October 2026, https://www.ashurstperkinscoie.com/en/insights/asics-first-comprehensive-review-of-sustainability-reports/
- AASB, AASB S2 Climate-related Disclosures, 20 September 2024, https://standards.aasb.gov.au/aasb-s2-sep-2024
- AASB, AASB S1 General Requirements for Disclosure of Sustainability-related Financial Information, 20 September 2024, https://standards.aasb.gov.au/node/3837
- AUASB, ASSA 5010 Timeline for Audits and Reviews of Information in Sustainability Reports under the Corporations Act 2001 (compiled, January 2026), https://www.auasb.gov.au/media/yffbehwp/assa-5010-timeline-for-audits-and-reviews-of-information-in-sustainability-reports-under-the-corporations-act-2001.pdf
- AICD, Climate reporting legislation passes Senate: reporting to commence from 1 January 2025, 2024, https://www.aicd.com.au/risk-management/framework/climate/climate-reporting-legislation-passes-senate-reporting-to-commence-from-1-january-2025.html
- BDO Australia, ASIC provides guidance on the modified liability settings for mandatory sustainability reporting, 2025, https://www.bdo.com.au/en-au/insights/esg-sustainability/asic-provides-guidance-on-the-modified-liability-settings-for-mandatory-sustainability-reporting

ON THE BOARD AGENDA

Cyber Risk for Boards: The Australian Picture at November 2026

By Sukh Sandhu

Cyber risk is now a standing item of corporate governance in Australia, shaped by government threat data, a changing control framework, mandatory reporting laws and clear expectations of directors. This article brings together the latest figures from the Australian Signals Directorate and the privacy regulator, explains the obligations that now apply, and ends with the questions every board should be asking management.

The threat picture: ASD's Annual Cyber Threat Report 2025 to 26

The Australian Signals Directorate (ASD) released its seventh *Annual Cyber Threat Report*, covering the 2025 to 26 financial year, in October 2026. The report names artificial intelligence as the defining force in the threat landscape over the year, with the important qualification that AI has not introduced new types of threats so much as amplified and accelerated existing ones, such as social engineering and impersonation.

The headline figures from ASD's Australian Cyber Security Centre (ACSC) are below.

Measure (2025 to 26)	Figure
Calls to the Australian Cyber Security Hotline	Over 37,500, down 12%
Cybercrime reports to ReportCyber	Over 82,000, about one every 6 minutes
Cyber security incidents responded to	1,524, up about 20%
Ransomware incidents responded to	139, consistent with last year
Notifications of potential malicious activity	More than 4,400, up almost 80%
Publicly reported vulnerabilities (CVEs)	Up 30%

What cybercrime costs a business

The average self-reported cost of cybercrime per report for businesses rose 16% overall to $93,500. The breakdown by size is striking.

Business size	Average self-reported cost per report	Change
Small	$55,400	Consistent with last year
Medium	$141,300	Up 45%
Large	$148,100	Down 27%
Individuals	$33,000	Consistent with last year

These are self-reported figures from people and businesses who chose to report, and ASD notes that most cybercrime is likely to go unreported. They are best read as an indicator of direction and scale rather than a full measure of loss. Even so, a jump of 45% for

medium businesses should catch the attention of boards in the mid market, where security budgets are often smallest relative to exposure.

Ransomware, data theft and critical infrastructure

ASD responded to 139 ransomware incidents in 2025 to 26. The number was steady, but severity increased: incidents classed as extensive rose from 16 to 24. Health care, professional, scientific and technical services, and manufacturing remained the three most affected industry divisions. ASD reminds organisations that paying a ransom does not guarantee recovery of data or prevent it being sold or leaked.

Data breaches recorded by ASD rose 66% to 98 incidents, more than 6% of all incidents. Critical infrastructure incidents made up 10% of all incidents, with ASD responding to 154, and phishing was the most common initial access technique in those incidents. Compromised accounts and credentials were among the most frequently reported incident categories across government, industry and critical infrastructure, which is why ASD continues to push stronger authentication such as multi-factor authentication and passkeys.

From the Essential Eight to the Essentials series

Since 2017 the Essential Eight has been the best known Australian baseline for cyber security. It consists of eight mitigation strategies:

1. patch applications;
2. patch operating systems;
3. multi-factor authentication;
4. restrict administrative privileges;
5. application control;
6. restrict Microsoft Office macros;
7. user application hardening;
8. regular backups.

The accompanying maturity model defines levels from Maturity Level Zero to Maturity Level Three, each aimed at a progressively more capable adversary. Many Australian organisations, and many government contracts and regulators, have measured cyber posture against these levels.

In October 2026 the ACSC released the **Essentials series**, which ASD describes as the evolution of the Essential Eight into a broader, principles based framework offering prioritised, threat informed mitigations with technology specific content. It was initially published in three chapters: Enterprise IT, Operational Technology and Cloud. ASD states that the Essential Eight remains effective, that organisations' investment in the Essential Eight maturity model is not discarded and can be carried forward, but that the mitigations and how they are measured have evolved and in many cases apply more broadly. ASD has said it will continue to engage with stakeholders on transitional arrangements into 2027.

For boards, this is a moment to ask an informed question rather than a technical one. If the organisation reports its posture as an Essential Eight maturity level, management

should explain how that maps to the new Essentials series, what changes for operational technology and cloud environments, and what the transition plan is. Contracts, insurance questionnaires and regulatory filings that reference Essential Eight maturity levels may also need review over the coming year.

Notifiable Data Breaches: the privacy regulator's numbers

The Notifiable Data Breaches (NDB) scheme under the *Privacy Act 1988* has applied since 2018. Entities covered by the Act must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) of an eligible data breach, which is unauthorised access to, disclosure of or loss of personal information that is likely to result in serious harm. Where an entity suspects an eligible breach, it must take reasonable steps to complete an assessment within 30 days.

The latest OAIC statistics, released on 26 October 2026, cover January to June 2026.

NDB measure	Figure
Notifications, January to June 2026	667
Notifications, July to December 2025	662
Breaches affecting more than 1 million people	11, up from 4
Calendar year 2025 total	1,205, the highest annual total since the scheme began

Malicious or criminal attacks remained the leading source of breaches. The health sector notified the most breaches (149), followed by education (85), business and professional associations (79), and financial services and personal services (51 each). The OAIC also reported that more than half of breaches were identified within 10 days, and that the share taking over 30 days to identify had declined.

Privacy Commissioner Carly Kind put the main lesson simply: "Organisations can't lose personal information they don't hold." For boards, data minimisation and retention are not only privacy questions. They are among the most effective ways to reduce the consequences of a cyber incident.

Ransomware payment reporting under the Cyber Security Act 2024

The *Cyber Security Act 2024* received Royal Assent on 29 November 2024. Part 3 of the Act introduced mandatory reporting of ransomware and cyber extortion payments, which commenced on 30 May 2025.

The key elements, as set out by the Department of Home Affairs, are:

- **Who must report.** A reporting business entity is one carrying on business in Australia with annual turnover for the previous financial year exceeding $3 million (with a pro rata formula for part years), or a responsible entity for a critical infrastructure asset to which Part 2B of the *Security of Critical Infrastructure Act 2018* applies. Commonwealth and State bodies are excluded. Not for profit organisations are not expressly exempt.

- **What triggers a report.** A report is required when the entity makes a ransomware or cyber extortion payment, or becomes aware that a payment has been made on its behalf. Payments can be monetary or non-monetary. A demand that is not paid does not trigger the mandatory obligation, although voluntary reporting is encouraged.
- **When.** The report must be made to ASD within 72 hours of the payment, or of becoming aware of it.
- **Phasing.** Home Affairs ran an education first approach from 30 May 2025 to 31 December 2025, pursuing regulatory action only for egregious non-compliance. From 1 January 2026, it moved to a compliance and education phase with a more active regulatory focus.

The obligation does not make paying a ransom unlawful, and it does not change the Government's advice against paying. What it does is make the payment decision visible. In our view, a board should decide in advance, as part of incident planning, who has authority to approve or reject a payment, what legal and sanctions advice is required, and who makes the 72 hour report.

The Security of Critical Infrastructure Act in outline

The *Security of Critical Infrastructure Act 2018* (SOCI Act), administered by the Cyber and Infrastructure Security Centre within the Department of Home Affairs, applies to responsible entities for assets in 11 critical infrastructure sectors, including energy, water, communications, financial services, health care, transport and data storage. The obligations depend on the asset class, but in outline they include:

- **Register of critical infrastructure assets.** Providing ownership and operational information to Government.
- **Mandatory cyber incident reporting.** Reporting cyber security incidents to ASD within 12 hours for incidents having a significant impact on the availability of an asset, and within 72 hours for incidents having a relevant impact.
- **Critical infrastructure risk management program (CIRMP).** Adopting and maintaining a program that identifies and mitigates material risks across cyber and information security, personnel, supply chain, and physical and natural hazards. The CIRMP Rules commenced on 17 February 2023.
- **Annual CIRMP report.** Submitting an annual report on the program to the regulator within 90 days after the end of each Australian financial year (that is, by 28 September). If the entity has a board, council or other governing body, the report must be approved by it before submission.
- **Enhanced cyber security obligations.** Additional requirements, such as incident response planning, exercises and vulnerability assessments, for assets declared systems of national significance.
- **Government assistance.** Powers for Government to direct or assist in serious incidents as a last resort.

The annual board approval requirement is the point that brings SOCI into the boardroom directly. A board that signs a CIRMP annual report should understand what it is attesting to, and should have seen evidence, not just a summary.

What good governance looks like

Two sources of guidance are especially useful for Australian directors.

The AICD and CSCRC Cyber Security Governance Principles

The Australian Institute of Company Directors (AICD) and the Cyber Security Cooperative Research Centre (CSCRC) first published the *Cyber Security Governance Principles* in October 2022 and released Version 2 on 25 November 2024. The refresh added material on digital supply chain risk, data governance, incident response and recovery, and regulatory change. The principles are organised under five themes:

1. clear roles and responsibilities for the board and management;
2. a comprehensive cyber strategy, developed, implemented and evolved over time;
3. cyber security embedded in existing risk management practices;
4. a culture of cyber resilience;
5. planning for a significant cyber security incident.

The principles include questions for directors, red flags, and checklists for small and medium enterprises and not for profits.

ASD and AICD board priorities

In late 2025 ASD and the AICD published *Cyber security priorities for boards of directors 2025 to 26*. It identifies four priority areas and sets out threshold questions for boards to ask management:

- event logging and threat detection;
- management of legacy information technology;
- cyber supply chain controls;
- preparing for a post-quantum cryptography environment.

ASD's 2025 to 26 threat report repeats those priorities and points to stopping the use of traditional asymmetric cryptography by the end of 2030, or sooner, as part of post-quantum readiness. The AICD acknowledges that many small and medium enterprises and not for profits will not be able to follow all of the advice, which is a reasonable reminder that proportionality applies.

Directors' duties and cyber

Directors owe duties of care and diligence under section 180 of the *Corporations Act 2001*. ASIC has repeatedly said that directors should treat cyber risk as part of their oversight responsibilities, has identified cyber resilience as an enforcement priority, and has taken court action against financial services licensees for failing to manage cyber security risk adequately. In our view, the practical standard for a director is not technical expertise. It is informed oversight: understanding the organisation's most important systems and data, knowing the material risks, asking whether controls are working, and making sure the organisation can respond when they fail.

What good board reporting looks like

Many boards receive cyber reporting that is long on activity and short on insight: counts of blocked emails, patching percentages without context, and traffic light dashboards that are always amber. In our view, useful cyber reporting to a board has five features.

Feature	What it shows
Risk focus	The top cyber risks to the most important systems and data, and how they are changing
Control effectiveness	Whether key controls are working, with independent testing where possible
Trend and benchmark	Movement over time, and comparison with a recognised framework
Incidents and near misses	What happened, what was learned and what changed
Decisions required	Investment, risk acceptance or policy choices the board needs to make

Internal audit has a valuable role here. An independent review of the accuracy of cyber reporting, or of a sample of the controls it claims are in place, gives directors a basis for relying on what they are told.

The board questions checklist

The questions below draw on the AICD and CSCRC principles, the ASD and AICD board priorities, and the obligations discussed above. They are a starting point for a board discussion with management, not a substitute for specialist advice.

Strategy and accountability

1. Who on the executive team is accountable for cyber security, and do they have the authority and budget to act?
2. Which committee oversees cyber risk, how often does it receive reporting, and does that reporting include trends, not just activity?
3. What are our crown jewels: the systems, services and data whose loss would most harm customers or the business?

Controls and posture

1. What is our current maturity against the Essential Eight, and what is the plan to transition to the Essentials series for enterprise IT, operational technology and cloud?
2. Is phishing resistant multi-factor authentication in place for remote access, administrators and email?
3. Which legacy systems are internet facing or out of support, and what is the plan to retire or isolate them?
4. Are we collecting and retaining the logs needed to detect and investigate an incident, and is someone reviewing alerts?

Data and privacy

1. What personal information do we hold that we no longer need, and when will it be deleted?

2. Could we complete an NDB assessment within 30 days, and who decides whether a breach is notifiable?

Supply chain

1. Have critical suppliers been tiered by risk, and have their security controls been assessed or certified?
2. Do our contracts require suppliers to notify us of incidents promptly and support our investigation?

Incident readiness

1. Do we have a tested incident response plan, and when did the board last take part in an exercise?
2. If we were extorted, who would decide on a ransom payment, what advice would we take, and who would make the 72 hour report if we paid?
3. If we are a SOCI responsible entity, can we meet the 12 hour and 72 hour reporting deadlines, and what evidence supports our CIRMP annual report?
4. Are our backups isolated, tested, and able to restore critical services within an acceptable time?

What to do this month

1. **Ask for the briefing.** Request a short management briefing on the ASD 2025 to 26 threat report and what it means for your sector and size.
2. **Ask about the Essentials series.** Ask management how the October 2026 release of the Essentials series affects your control framework, contracts, insurance and any regulatory reporting.
3. **Check the ransomware decision path.** Confirm that your incident plan names who can approve or reject a payment and who will lodge the report with ASD within 72 hours.
4. **Review data holdings.** Ask for a list of the largest personal information data sets you hold and the retention rule for each.
5. **Schedule an exercise.** If the board has not taken part in a cyber incident exercise in the past 12 months, book one.
6. **Use the checklist.** Put the board questions above to management and record the answers and actions in the minutes.

The bottom line

The Australian data points in a consistent direction. Cybercrime reporting is steady at roughly one report every six minutes, costs for medium businesses have jumped, large data breaches are increasing, and AI is making familiar attacks faster and more convincing. At the same time, the rules have firmed: ransomware payments must be reported, critical infrastructure boards must approve risk management reports, and ASD has modernised its core control framework. In our view, the boards that handle this well will be the ones that ask clear questions, insist on evidence, and practise their response before they need it.

Sources

- Australian Signals Directorate, Annual Cyber Threat Report 2025-26, October 2026, https://www.cyber.gov.au/sites/default/files/2026-10/Annual%20Cyber%20Threat%20Report%202025-26.pdf
- Australian Signals Directorate, ASD releases seventh annual Cyber Threat Report 2025-26, October 2026, https://www.cyber.gov.au/news/asd-releases-seventh-annual-cyber-threat-report-2025-26
- Office of the Australian Information Commissioner, Large scale data breaches on the rise, latest OAIC statistics reveal, 26 October 2026, https://www.oaic.gov.au/news/media-centre/large-scale-data-breaches-on-the-rise,-latest-oaic-statistics-reveal
- Office of the Australian Information Commissioner, Data breach notifications increase to all time high in 2025, new NDB stats show, 2026, https://www.oaic.gov.au/news/media-centre/data-breach-notifications-increase-to-all-time-high-in-2025,-new-ndb-stats-show
- Federal Register of Legislation, Cyber Security Act 2024, assented 29 November 2024, https://www.legislation.gov.au/C2024A00098/asmade/text
- Department of Home Affairs, Factsheet: Mandatory ransomware and cyber extortion payment reporting is active from 30 May 2025, https://www.homeaffairs.gov.au/cyber-security-subsite/files/factsheet-ransomware-payment-reporting.pdf
- Cyber and Infrastructure Security Centre, Security of Critical Infrastructure Act 2018 obligations, https://www.cisc.gov.au/
- Maddocks, Annual reporting requirements for your critical infrastructure risk management program, 2024, https://www.maddocks.com.au/insights/annual-reporting-requirements-for-your-critical-infrastructure-risk-management-program
- Australian Institute of Company Directors and Cyber Security Cooperative Research Centre, Cyber Security Governance Principles Version 2, 25 November 2024, https://www.aicd.com.au/risk-management/framework/cyber-security/cyber-security-governance-principles.html
- Australian Signals Directorate, Cyber security priorities for boards of directors 2025-26, October 2025, https://www.cyber.gov.au/business-government/protecting-business-leaders/cyber-security-for-business-leaders/cyber-security-priorities-for-boards-of-directors-2025-26
- Australian Institute of Company Directors, ASD and AICD guidance on board cyber priorities for 25/26, November 2025, https://www.aicd.com.au/board-of-directors/performance/effectiveness/asd-and-aicd-guidance-on-board-cyber-priorities-for-25-26.html

BACK PAGE

About RiskWise

RiskWise is an independent monthly magazine for boards, audit committees, auditors and risk professionals: the standards, the regulation and the practice of audit, risk and assurance. It is one of a family of independent titles: LeadWell, RiskWise, How They Rose, Wiser Days and TeachWise.

Contribute

Tell us about a risk or assurance question you would like examined. Write to sukh@sukhsandhu.com.

Disclaimer

This publication provides general information only. It is not legal, financial, investment, medical, migration or regulatory advice. Check current requirements with the relevant regulator, department or a qualified adviser before acting. Information is current at November 2026; fees, thresholds and figures change, so check each source before relying on it.

Copyright

Copyright Sukh Sandhu 2026. All rights reserved. No part of this publication may be reproduced without the publisher's written permission, except as permitted under the Copyright Act 1968 (Cth). Material quoted from Australian Government publications is used under the terms of their licences, including Creative Commons Attribution 4.0 where stated by the publishing body.

RiskWise | riskwisemag.com | sukh@sukhsandhu.com

Masthead

Publisher: RiskWise

Editor-in-Chief: Sukh Sandhu

Edition: Edition 1 | December 2026

Website: riskwisemag.com

Contributions, corrections and enquiries: sukh@sukhsandhu.com

Sister titles: LeadWell, RiskWise, How They Rose, Wiser Days and TeachWise

RiskWise explains audit, risk and assurance for directors, audit committees, internal and external auditors and risk managers. Standards and laws are named and dated. Nothing in this magazine is legal, accounting or audit advice.