Shape the future with confidence

ASIC signals urgency on AI-accelerated cyber risk

ASIC open letter on frontier AI and cyber resilience

Governance must keep pace with evolving risks

The better the question.
The better the answer.
The better the world works.

At a glance

On 8 May 2026, ASIC Commissioner Simone Constant issued a letter calling for greater action on cyber resilience in the face of AI-accelerated threats.

- **What's changed:** AI is increasing the speed, scale and accessibility of cyber attacks.
- **What ASIC expects:** Board and senior executive oversight supported by evidence-based assurance.
- **What you should do now:** Reassess plans, strengthen fundamentals, validate controls.

What risks do frontier AI models pose?

The Australian Securities and Investments Commission's (ASIC) letter says frontier AI models are accelerating both capability and accessibility, increasing the speed and scale of attacks, and enabling new forms of exploitation. Attacks will happen faster, on a greater scale and with fewer barriers to entry. Techniques and capabilities that were previously out of reach for many actors are becoming more accessible, more rapidly deployed and harder to manage using business-as-usual approaches. Small gaps in controls will be exposed more quickly and more severely.

For regulated entities, this creates a more demanding operating environment in which small control weaknesses can have more serious and cascading consequences. The implication is that management teams need to anticipate a more intense, faster-moving threat environment in which patching delays, privileged access weaknesses, untested response plans and third-party dependencies may be exposed more quickly and exploited more effectively. This is in addition to increased insider threats, and calls for monitoring warning signs and restricting access where concerns are identified.

This also aligns with broader regulatory signals, including the recent Five Eyes cyber security agencies statement and the Australian Prudential Regulation Authority (APRA) open letter to industry signalling that AI-related risk management is now considered by regulators as a board-level governance, accountability and resilience issue.

What does the letter say?

ASIC has delivered a clear message to licensees and directors: frontier AI models mark a significant shift in the cyber threat landscape by increasing the capability and accessibility of sophisticated cyber activity, accelerating the speed and scale of attacks and enabling new forms of exploitation. ASIC's message is clear: this is not a distant or hypothetical issue. It is here now, evolving quickly, and requires the attention of boards and executives.

The letter does not suggest that frontier AI creates entirely new categories of risk. Rather, ASIC's point is that existing controls are more likely to be tested, more often and under greater pressure. Its message is to act now, with urgency and discipline, to strengthen the cyber resilience fundamentals that underpin the business.

ASIC is not calling for panic or reactive overreach. Instead, it is calling for urgency, focus and accountability, with a practical emphasis on core cyber resilience measures, clear governance, adequate resourcing and evidence-backed assurance.

Importantly, ASIC expects the letter to be tabled and discussed at ultimate board and risk governance committees, underlining that this is not just a technology or security issue, but a leadership and governance issue.

Sources:
ASIC Letter on AI-accelerated cyber threats
APRA open letter to industry on Artificial Intelligence (AI)
Five Eyes cyber security agencies statement

What issues do you need to be aware of?

Reinforcing cyber resilience fundamentals

Strong cyber resilience is built on the consistent execution of well-established controls, supported by clear governance and adequate resourcing. In an AI-enabled threat environment, fundamentals such as patching, access management, network exposure reduction, and incident readiness become more important, while boards should remain open to innovative approaches where appropriate.

Critical asset and system protection

Organisations should identify and protect critical assets and systems, with a clear understanding of what matters most to the business and its customers. That implies a need for visibility over highly valuable systems, critical services and priority recovery targets.

Access and privilege management

Entities need to regularly review user access and reassess privileges to protect against unauthorised access. Entities also need to monitor for insider threats and other warning signs, and restrict access where concerns arise.

Patching and vulnerability management

Recognising that AI is accelerating vulnerability discovery and exploitation, entities should patch promptly. Patch management processes, including dealing with the identification, testing and governance challenges associated with frequent critical updates, also need to be strengthened.

Defence-in-depth and attack surface reduction

Minimise attack surfaces by reducing exposure of systems and services to untrusted networks, and implement layered, defence-in-depth architectures that assume breach and restrict lateral movement.

Incident response and business continuity readiness

Organisations should maintain and exercise incident response plans and playbooks, including business continuity planning and identification of highest-priority services, channels and platforms. This makes operational readiness a central theme of the letter, elevating its importance beyond compliance considerations.

Third-party and concentration risk

ASIC also calls for active management of third-party risks, particularly where services introduce concentration or systemic exposure. This aligns with the broader regulatory concern that AI-related supplier dependency and concentration risks are becoming more significant.

Evidence-backed governance

Governance should not rely only on assurances. ASIC says it should be supported by evidence such as test results, audit findings, lessons from incidents and independent validation. Boards and executives are expected to receive meaningful reporting on end-to-end control effectiveness, not just activity.

What this means for boards and senior executives

ASIC's letter makes it clear that cyber resilience is a leadership issue, not just an operational one. Cyber resilience is being treated as a core part of the obligations of licensees and market participants, and ASIC expects boards and senior executives to understand their organisation's position, ask the right questions, and evidence the basis for their assurance.

For boards and executive teams, that means oversight should be practical, informed and evidence-led. Leadership should be satisfied that cyber resilience measures are proportionate to the evolving threat environment, that cyber capability is adequately resourced and qualified, and that reporting focuses on end-to-end control effectiveness rather than activities alone.

It also means governance cannot stop at receiving management assurances. ASIC explicitly calls for evidence in the form of testing outcomes, audit findings, lessons from incidents and independent validation. This reinforces a broader regulatory expectation that boards are expected to demonstrate active oversight and evidence-based assurance as AI adoption and AI-enabled threats accelerate.

At the same time, the message is to focus on ensuring that the foundational elements are robust, resourced and working effectively. For leadership teams, the implication is clear: strengthen foundations, improve visibility, test readiness, and ensure the organisation can demonstrate that controls are operating effectively under pressure.

Key questions for boards, executives, and risk leaders

1. Have we reassessed our cyber plans in light of the way frontier AI is changing the threat landscape, or are we still relying on assumptions better suited to a slower-moving environment?
2. Do we have a clear view of the critical assets, systems, services and data that matter most to our business and customers, and are they being protected accordingly?
3. Are our core cyber controls demonstrably effective, or are we taking comfort from activity and process without clear evidence of control performance?
4. How quickly can we identify, assess, test and deploy critical patches in an environment where vulnerabilities may be discovered and exploited more rapidly?
5. Do our incident response and business continuity plans reflect our highest-priority services, channels and platforms, and are they regularly exercised in practice?
6. Is the board receiving meaningful reporting on end-to-end control effectiveness, supported by testing, audit findings, incident lessons and independent validation?

Immediate priorities

Reassess cyber strategy for AI-enabled threats

Management teams should revisit cyber plans and refocus effort on the most critical risks in the current threat environment, rather than waiting for more certainty or more mature standards.

Confirm governance and decision-making are fit for pace

Cyber risk, governance and broader risk and decision-making frameworks should reflect the cumulative effect of interrelated vulnerabilities and support clear escalation and timely decisions.

Protect critical assets and systems

Organisations should ensure they have a clear understanding of their most critical assets and systems and prioritise those assets for protection, resilience and recovery.

Validate control effectiveness

Regular review and validation of fundamental controls should be an immediate priority, including attack surface reduction, access and privilege review, patching discipline and layered security architecture.

Test incident response under pressure

Incident response plans and playbooks should be maintained, exercised and aligned to the organisation's highest-priority services and channels so they can be relied on during a significant event.

Re-evaluate third-party exposure

Third-party services, including dependencies that may create concentration or systemic exposure, should be reviewed.

Strengthen evidence-based assurance

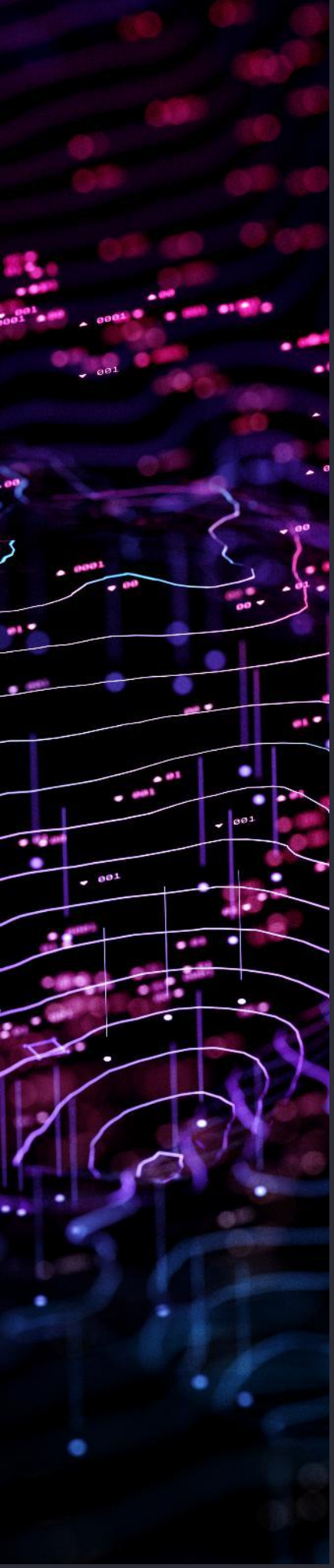
Boards and executives should expect evidence-based assurance that draws on testing, audit results, lessons from incidents and independent validation, rather than relying on high-level comfort statements.

How EY teams can help

Our EY teams can support organisations with AI governance assessments, cyber resilience reviews and board and executive scenario testing through practical scenario exercises.

We help boards, executives and management teams assess whether cyber resilience arrangements remain proportionate in a changing AI-enabled threat environment, identify the most significant control and governance gaps for review, and prioritise practical uplift actions that can withstand regulatory, board and stakeholder scrutiny.

We also support organisations in advancing from periodic assurance to more defensible and continuous assurance over cyber resilience, third-party risk, governance effectiveness and operational readiness, particularly as AI increases the pace and complexity of the risk environment.



How we can support you across the cyber and AI resilience lifecycle

AI governance maturity assessment

We help organisations assess how mature their AI governance is today and what needs to improve to support safe, scalable and defensible AI adoption. The EY AI Governance Maturity Assessment evaluates current-state maturity across nine AI governance domains through stakeholder interviews, control walkthroughs and document reviews, and translates the findings into prioritised gaps, target-state maturity and a practical roadmap for uplift.

AI data readiness and quality

We help clients determine whether the data underpinning their AI use cases is accurate, complete, reliable and fit for purpose before it is used in models or operational AI systems. The EY AI Data Readiness Assessment assesses readiness across the AI data lifecycle, including data strategy, quality, management, ownership, infrastructure, governance and compliance, while related AI data quality testing services can provide deeper validation of in-scope data for AI training and operations.

AI crisis simulation and incident readiness

We help boards and executive teams test how prepared they are to respond to an AI-related incident before a real event occurs. The EY Board Response Simulation: AI Crisis is an interactive exercise that helps organisations identify gaps in crisis management plans, increase leadership awareness of AI-related risks, and strengthen resilience in the face of issues such as AI-generated inaccuracies, bias and cyber security vulnerabilities.

AI cyber security and resilience readiness

We support organisations with cyber resilience reviews, governance assessments and readiness testing relevant to AI-enabled threat conditions. We can support across AI workshops, risk and security assessments, roadmaps, architecture and guardrails and AI-enabled cyber-operations, including threat detection and response. Related EY cyber engineering capabilities also support more secure deployment through stronger access controls, protected credentials, human-AI workflows and greater traceability across cyber activities.

EY Contacts:

Christina Larkin
EY Regional Digital Assurance Leader, Oceania
christina.larkin@au.ey.com

Richard Bergman
EY Global Cyber Security Transformation Leader
richard.bergman@au.ey.com

Jason Knott
EY Assurance Forensic & Integrity Services Partner
jason.Knott@au.ey.com

Services are subject to applicable independence, conflict and permissibility requirements.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fuelled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

AU SCORE no. 112975-26-AUNZ

ED None

ey.com