Australian Securities and Investments Commission

Office address (inc courier deliveries):

Level 7, 120 Collins Street,
Melbourne VIC 3000

Mail address for Melbourne office:

GPO Box 9827,
Melbourne VIC 3001

Tel: +61 1300 300 630
www.asic.gov.au

8 May 2026

Licensees and directors,

The rapid evolution of frontier artificial intelligence models marks a significant shift in the cyber threat landscape. These models are accelerating both capability and accessibility, lowering the barrier to sophisticated cyber activity, increasing the speed and scale of attacks, and enabling new forms of exploitation that were previously out of reach for most actors.

This does not mean entirely new categories of risk, but it does mean existing controls are more likely to be tested, more often, and under greater pressure.

This is not a distant or hypothetical risk. It is here now, evolving quickly and requires the attention of boards and executives.

ASIC's message is straightforward: **do not wait for perfect clarity to address the threat posed by new AI models. Instead, act now, and act with discipline, to strengthen the cyber resilience fundamentals that underpin your business.**

We are not calling for panic or reactive overreach. But we are calling for urgency, focus, and accountability.

A clear call to action: Focus on what matters - cyber resilience basics

In this environment, ASIC expects entities to return to first principles. Strong cyber resilience is not built on novel tools.

As set out in the court's judgment in ASIC's case against FIIG Securities Limited, cyber risk management must be demonstrably effective and proportionate to the size, nature and complexity of a business (26-021MR). It is built on consistent execution of well-established controls, supported by clear governance and adequate resourcing.

We encourage you to take the following steps now:

- **reassess your cyber plans** and refocus efforts on the most critical risks in today's threat environment.
- **confirm your cyber risk, governance and overall risk and decision-making frameworks** consider the cumulative impact of interrelated vulnerabilities and facilitate clear decision making and escalation at the pace necessary to manage risk.
- **identify and protect critical assets and systems,** with a clear understanding of what matters most to your business and customers.
- **strengthen cyber security fundamentals** by regularly reviewing and validating core controls.

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

These are not new expectations, but the environment in which they must operate has changed. Small weaknesses can have serious, cascading consequences. For example, a 'simple' phishing email can now more easily provide access to critical platforms or sensitive data, and a weakness that in isolation may be remote from being a conduit for a cyber incident can now more readily be drawn together with other weaknesses into an incident. Strengthening the basics is imperative, as they shape the baseline for your overall resilience.

Governance and accountability remain critical

Cyber resilience is a core part of your obligations as a licensee and market participant. ASIC expects boards and senior executives to understand their organisation's position, ask the right questions, and be able to evidence the basis for their assurance. In practice, this includes:

- Being satisfied that cyber resilience measures are proportionate to the evolving threat environment.
- Ensuring cyber capability is adequately resourced, prioritised and qualified to the standard necessary for the services and risk footprint of your organisation.
- Receiving meaningful reporting on end-to-end control effectiveness, not just activity.
- Overseeing how emerging risks, including those from AI, are being assessed and integrated into risk management frameworks.

Governance should not rely only on assurances. It should be supported by evidence - test results, audit findings, lessons from incidents, and independent validation, supported by appropriate capability and resourcing.

Too often cyber-attacks are successful because known vulnerabilities are exploited. ASIC's expects regulated entities to actively prepare for cyber incidents, respond

promptly and effectively when they occur, and recover in a way that restores critical services, minimises harm, and strengthens future resilience.

Use guidance that already exists

ASIC encourages entities to use the practical guidance from the Australian Signals Directorate (ASD), including their broader publications (e.g. ASD advice on emerging threats and the implications of new technologies) which offer actionable and current insights.

Further information is available at:

- https://www.cyber.gov.au
- Frontier models and their impact on cyber security

Entities may also wish to subscribe to ASD alerts and consider the ASD partnership program where appropriate.

ASIC's regulatory resources include further information about cyber security and cyber resilience: Cyber resilience good practices | Cyber risk: Be prepared | Resources on cyber resilience Entities may also wish to consider APRA's Letter to Industry on Artificial Intelligence

Final remarks

Frontier AI models are a step-change in capability, but they do not change the fundamentals of good cyber resilience; rather, they reinforce the importance of strong, end-to-end preparedness. Entities that have established robust plans across the full cyber incident lifecycle, and keep those plans current, tested and embedded, will be better placed to manage the accelerating threats posed by frontier AI.

ASIC will continue to monitor developments closely and engage with international regulators, Council of Financial Regulators agencies, Department of Home Affairs, Australian Signals Directorate and industry participants. We expect licensees to do the same.

Appropriate cyber risk management starts at the accountable leadership of licensees and participants. Please ensure this letter is tabled and discussed at your ultimate board and risk governance committees.

The time to act is now, not by reinventing your approach, but by ensuring the basics are robust, resourced, and working effectively.

Simone Constant
Commissioner
Australian Securities and Investments Commission