ASIC calls for cyber uplift

What AI-enabled cyber risk means for licensees

Iona Luke

On 8 May 2026, the Australian Securities and Investments Commission (ASIC) issued an open letter[1] to Australian financial services licensees and market participants calling for an urgent uplift in cyber resilience measures (the Letter). Issued against the background of growing concern about the impact of frontier AI on cyber risk, the Letter reinforces ASIC's expectations regarding cyber governance, operational resilience and risk management under existing licence obligations.

That message is consistent with broader warnings from the Australian Signals Directorate[2] regarding the impact of AI on cyber risk and the increasing accessibility of sophisticated cyber capabilities.

Existing obligations, evolving environment

For Australian financial services (AFS) licensees and Australian Credit Licence (ACL) holders, cyber resilience already forms part of existing obligations concerning the provision of financial services, adequate resources and risk management. What is changing is the threat environment in which those obligations must be met. As AI increases the capability and accessibility of sophisticated cyber attacks, the effectiveness of existing governance, risk management and operational resilience arrangements is likely to come under greater scrutiny.

The Letter is the latest step in ASIC's evolving approach to cyber risk management. ASIC's enforcement activity against RI Advice Group, Fortnum Private Wealth and FIIG Securities reflects an increasing focus on cyber risk management as a core licensing obligation. That focus is also evident in ASIC's Key Issues Outlook 2026, which identifies cyber attacks, data breaches and inadequate operational resilience as significant risks for regulated entities.

The Letter builds on that trajectory.

Table 1. ASIC enforcement actions and regulatory developments relating to cyber risk management

Development	What it means for licensees
ASIC v RI Advice Group Pty Ltd (2022)[3]	Cyber risk is a core operational risk that requires adequate risk management systems to manage.
Proceedings against Fortnum Private Wealth (2025 – ongoing)[4]	Having a documented framework is not enough; implementation and supervision matter.
ASIC v FIIG Securities Limited (2026)[5]	Adequate resources obligations extend to cyber risk management.
ASIC's Letter calling for cyber resilience uplift (2026)	Existing frameworks should be assessed against an evolving threat environment.

Source: Holley Nethercote

While each case arose on its own facts, it is notable that in both *RI Advice* and *FIIG Securities*, the Court found breaches of sections 912A(1)(a) and 912A(1)(h) of the *Corporations Act 2001* (Corporations Act), which require AFSL holders to do all things necessary to ensure that financial services are provided efficiently, honestly and fairly and to maintain adequate risk management systems. In *FIIG Securities*, the Court also found a breach of section 912A(1)(d), which requires AFSL holders to have adequate financial, technological and human resources to provide the financial services covered by the licence and carry out supervisory arrangements. Those decisions reinforce the proposition that inadequate management of cyber risks may give rise to breaches of core licence obligations.

ASIC's Letter encourages entities to focus on cyber resilience fundamentals and identifies a range of measures intended to strengthen cyber preparedness, governance and resilience. Those measures provide a useful indication of the matters ASIC considers relevant to managing cyber risk under existing licence obligations.

Governance, controls and risk management

A central theme of the Letter is that cyber risk is a governance issue requiring appropriate board and executive oversight and accountability. Licensees should consider whether accountability, reporting and escalation arrangements are sufficiently clear and responsive to enable cyber risks to be identified, escalated and addressed at the pace required by an increasingly complex threat environment.

More broadly, the measures identified in the Letter reflect ASIC's focus on how cyber risks are managed in practice. As the *FIIG Securities* proceedings illustrate, cyber risk management cannot be reduced to the existence of policies and controls alone. Risk management also requires organisations to understand whether those controls remain appropriate to the risks being managed and are operating as intended. In an AI-enabled environment, that may require ongoing reassessment of controls as threat capabilities evolve.

Operational resilience and third-party dependencies

The measures identified in the Letter relating to incident response and the identification of critical assets and systems reflect ASIC's expectation that licensees should be capable of responding to and recovering from cyber incidents effectively. This is particularly important where incidents affect systems, services or assets whose disruption could have a significant impact on customers or the delivery of financial services.

Strong incident response capabilities are also important from a compliance and governance perspective. They assist licensees to identify, assess and escalate potential breaches arising from cyber incidents, meet applicable regulatory reporting obligations within relevant timeframes, and make timely decisions regarding regulatory obligations arising from cyber events.

The Letter also recognises the increasing reliance of many organisations on external technology providers, including cloud and AI service providers. These arrangements can create operational dependencies and concentration risk, particularly where critical systems or services depend on a small number of providers. This makes supplier due diligence, ongoing oversight and appropriate contractual protections increasingly important components of cyber risk management.

ASIC's encouragement that entities consider whether AI can be used for defensive purposes is a reminder that frontier AI presents both risks and opportunities. The practical challenge for licensees is determining how AI-enabled tools can be incorporated into existing cyber security, governance and risk management frameworks in a way that enhances resilience without introducing unmanaged risks.

Looking ahead

In light of ASIC's Letter and broader enforcement activity, the key question for licensees is whether existing governance, risk management and operational resilience arrangements remain fit for purpose in an AI-enhanced threat environment. Licensees should expect increasing scrutiny not merely of whether frameworks and controls exist, but whether they are implemented, monitored and fit for purpose. Licensees should be prepared to demonstrate, through appropriate governance and operational evidence, that cyber risks are being actively managed and overseen in practice.

As AI continues to increase both the sophistication and accessibility of cyber threats, the challenge for licensees may be less about responding to a single technological development and more about ensuring that governance, risk management and operational resilience arrangements remain sufficiently adaptable to a threat environment that is evolving more rapidly than before. **FS**

Notes

1. ASIC, 26-092MR *ASIC calls for urgent cyber uplift as AI accelerates cyber threats*, 7 May 2026
2. Australian Signals Directorate, Australian Cyber Security Centre, *Five Eyes cyber security agencies publish guidance on identifying and mitigating AI-enabled cyber threats*, 22 Jun 2026
3. *Australian Securities and Investments Commission v RI Advice Group Pty Ltd* [2022] FCA 496
4. ASIC, 25-143MR *ASIC sues Fortnum Private Wealth for allegedly failing to adequately manage cybersecurity risks*, 22 July 2025
5. *Australian Securities and Investments Commission v FIIG Securities Limited* [2026] FCA 92

The quote

As AI increases the sophistication and accessibility of cyber threats, boards and executives should expect greater scrutiny of their cyber risk frameworks.

Iona Luke, Holley Nethercote

Iona is Special Counsel at Holley Nethercote and has deep experience in prudentially regulated financial services business, including senior legal and compliance roles at retail and wholesale banks, general and life insurers. She has a keen interest in privacy law, artificial intelligence and corporate governance. Iona is proficient in Cantonese and Mandarin.