Resilience at Frontier AI Speed

Insights from the APRA-ASIC Industry Roundtables

Joint publication | August 2026

APRA and ASIC expectations on managing Frontier AI risk

Frontier AI poses a real and present risk to Australia's financial system. It is accelerating known cyber, technology and operational risks, increasing the speed, scale and sophistication of cyber threats and creating the potential for unintended actions and outcomes from increasingly autonomous agentic systems.

In response to this growing risk, APRA and ASIC, in April and May respectively issued public letters outlining their expectations of regulated entities regarding frontier AI preparedness.[1] These letters emphasised the criticality of entities acting now to identify, understand and manage the risks created and amplified by frontier AI.

To support the industry in navigating this dynamic and rapidly evolving risk environment, and in keeping with our commitment to better regulation, APRA and ASIC have proactively collaborated to run a series of industry 'Frontier AI Roundtables'. This publication summarises the key insights derived from the roundtables to accelerate industry uplift.

Roundtables at a glance

9 roundtables | 600+ attendees | 380+ entities | regulated entities and non-regulated material service providers | industry associations representing more than 70,000 members

In June and July 2026, APRA and ASIC organised nine roundtables across industry, comprising over 380 entities and 600 attendees, to understand how entities are responding to frontier AI risks.

Participants comprised financial entities of all sizes, including banks, insurers, superannuation trustees, financial market infrastructure, market intermediaries, payment providers, financial services firms, mortgage brokers, financial advisers, investment managers, aggregators, credit providers, industry associations and our regulated entities' material service providers.

The roundtables were supported by the Australian Signals Directorate (ASD) and included participation from the Reserve Bank of Australia (RBA), Treasury and the Australian Competition and Consumer Commission (ACCC), signalling a whole-of-government response to this urgent threat.

Executive Summary

This was the first time that APRA and ASIC created rapid information-sharing forums across such a broad cross-section of the financial services industry. They were welcomed by industry as a practical and innovative way of sharing insights and better practice at scale, to support the resilience of the financial system.

The key message from the roundtable participants was that the financial services industry needs to move from awareness of frontier AI risk to action. For boards and executives, the question is no longer whether entities understand frontier AI risk. It is whether their entities can make decisions, maintain critical operations and recover when incidents unfold faster, affect more parties and involve

[1] APRA Letter to Industry on Artificial Intelligence (AI)
Media Release (26-092MR) ASIC calls for urgent cyber uplift as AI accelerates cyber threats

more complex dependencies. Participants spoke about an increasing urgency to match awareness with evidence of implementation, practical testing and measurable resilience outcomes.

Participants also recognised the important role that they play in the broader financial system and the need to clearly demonstrate how they are preparing for frontier AI. This includes demonstrating they can respond and recover under compressed timeframes while still meeting governance, cyber security, operational resilience and third-party risk management obligations. For critical market infrastructure providers, the roundtables highlighted the importance of enhancing the resilience of systems and processes that are relied upon by entities or groups of entities across the economy and markets more broadly.

Frontier AI risk traverses firms, markets, providers and borders, and participants reflected that effective industry collaboration will be critical to building resilience. The roundtables provided an opportunity for some larger entities to actively share their insights and resources with less well-resourced and smaller entities, and APRA and ASIC welcome this 'Team Australia' mindset. This type of practical collaboration and shared preparedness will be vital to maintaining the stability of our financial system.

Key themes from the roundtables

Across the nine roundtables, a number of key insights emerged. These may prove useful for entities as they work to strengthen their cyber preparedness.

Frontier AI raises the cost of weak cyber fundamentals

The roundtable discussions unanimously reinforced the importance of getting the cyber fundamentals right and demonstrating that these controls remain effective in a faster, more volatile, AI-enabled threat environment.

This includes visibility of technology resources and attack surfaces, timely patching, identity and access controls, monitoring, backup integrity, recovery arrangements and understanding where legacy systems may create vulnerabilities, constrain recovery options or complicate incident response. Appendix 1 provides a range of resources that can support entities in strengthening their cyber resilience and frontier AI preparedness.

Governance and escalation are pressure points

Participants noted they'd seen an increase in engagement from boards about the threats posed by frontier AI, with Anthropic's blog post regarding the risks associated with its Mythos model acting as a crystallising moment for many. They emphasised the importance of effective incident plans, escalation triggers, delegation arrangements and board involvement in decision-making. It was acknowledged that weaknesses in these settings could be as disruptive as technical control weaknesses.

It was recognised that under compressed incident response timeframes, entities may have limited opportunity to escalate decisions or resolve competing priorities. Participants emphasised the need for board decisions and guardrails to be put in place ahead of a crisis, such as those relating to risk appetite, escalation authority, supplier reliance, recovery priorities, communication strategies and resilience investment. Appendix 2 provides examples of some key questions that participants felt boards and executives should be asking themselves.

Defensive AI is promising, but still developing

Participants identified growing interest in defensive AI to strengthen capabilities such as threat intelligence, vulnerability detection, code review and incident response. However, it was acknowledged that governed, measurable and scalable defensive AI capability remains limited, and participants consistently noted that this is not a substitute for strong cyber fundamentals.

It was acknowledged that advanced capabilities will be required to harness more complex models, and like any critical capability, defensive AI requires governance, accountability, secure configuration, monitoring, reliability testing and human oversight. Poorly governed defensive AI introduces new risks, even when deployed with good intentions.

Shared dependencies can amplify disruption

The roundtables highlighted that common dependencies and concentration risk associated with third-party service providers can turn isolated individual incidents into much broader sector wide disruption that would have an amplifying impact on confidence in the financial system. This includes common reliance on cloud, Software as a Service, managed service providers, AI model providers, open-source components, payments infrastructure and telecommunications.

Participants highlighted the need to prove disruption readiness by understanding which providers and platforms support critical operations, where common dependencies exist, how disruption could spread, and whether fallback, restoration and reconnection arrangements work under compressed timeframes.

Collaboration is now part of resilience

Australia's financial system is highly interconnected, which can both amplify disruption and strengthen resilience through information sharing and coordination.

Participants saw the importance of actively contributing to industry- led collaboration, such as through industry associations, including sector-wide threat intelligence sharing, dependency mapping, supplier assurance and sector incident coordination. Whilst this would not replace any individual entity's own accountabilities and obligations, it can complement their resilience work. More advanced entities were eager to share practical insights, lessons and approaches with peers and less mature entities, and have arranged practical workshops following the engagements. This was encouraging, as resilience can be constrained by the least prepared parts of the ecosystem.

From awareness to action – what entities should do next

The roundtables have shown a high and growing level of awareness across industry that frontier AI has the potential to alter the speed, scale and complexity of cyber and operational disruption. The challenge now for entities, and industry as a whole, is to convert that awareness into tested governance, resilient operations and practical preparedness.

As set out in APRA's and ASIC's letters, the regulators expect entities to take action now to lift their resilience and to demonstrate that key decisions, escalation pathways, recovery arrangements, assurance activities and governance processes can operate at the speed required by emerging frontier AI threats. Preparedness for what lies ahead will depend on whether entities have built and tested the necessary resilience before disruption occurs, and this will continue to be a heightened focus of APRA and ASIC.

Appendix 1: Australian Government cyber resources

Entities may consider the following resources when assessing and strengthening their frontier AI preparedness:

APRA

- APRA Prudential Standard CPS 230 Operational Risk Management
- APRA Prudential Standard CPS 234 Information Security

ASIC

- ASIC Cyber resilience and operational resilience publications

Australian Signals Directorate

Australian Cyber Security Centre's guidance (ACSC) provides practical, proportionate actions for entities at different levels of maturity. The full set of ACSC's resources can be found at Cyber.gov.au:

- Five Eyes cyber security agencies statement
- Frontier AI Cyber Threat Considerations for Boards of Directors
- Defending against AI-enabled cyber attacks – guidance for government, critical infrastructure and large enterprises
- Essential Eight maturity model
- Information security manual
- Opportunities for AI in cyber defence
- Careful adoption of agentic AI services
- Artificial intelligence and machine learning: Supply chain risks and mitigations
- When AI agents take unexpected actions

Australian organisations that have been, or may be impacted by a cyber security incident, are encouraged to reach out to the Australian Signals Directorate (ASD). ASD's Australian Cyber Security Centre (ACSC) is the Australian Government's technical authority on cyber security.

- Supporting Australian organisations through a cyber security incident

ACCC

Entities that want to pursue an arrangement which involves sharing of commercially sensitive information, or other forms of coordination between them that may raise competition law risks, should seek an exemption from competition laws by lodging an authorisation application with the ACCC:

- ACCC Exemptions Process
- ACCC Authorisations

Other

- Trusted Information Sharing Network
- Small Business Cyber Resilience Service

Appendix 2: Preparedness topics from roundtables

Focus area	Example board questions	Evidence of preparedness
Governance and decision-making	• Have key escalation, shutdown, recovery and communications decisions been made before an incident occurs? • Have these decisions been tested under pressure? *If key decisions would be debated for the first time during an incident, this should be treated as a priority gap.*	Clear decision-making authority, tested escalation pathways, crisis exercises and evidence that frontier AI has influenced governance, risk appetite or investment decisions.
Cyber fundamentals	• Can critical vulnerabilities be identified, prioritised and remediated quickly enough? • Have recovery arrangements been tested against faster attack timelines? • Are any AI-enabled security tools governed, reliable and subject to human oversight? *Start with controls that affect critical operations, privileged access, recovery and services most exposed to rapid exploitation. While defensive AI may have an emerging role, this is not a substitute for strong cyber fundamentals.*	Tested backup and recovery arrangements, strong identity controls, effective monitoring and evidence that vulnerabilities are remediated within acceptable timeframes.
Critical dependencies and concentration risk	• Do we know which providers support our critical operations? • What happens if a common provider fails? *Prioritise dependencies that support critical operations, are hard to substitute, or are shared across multiple entities or markets.*	Dependency maps, concentration assessments, tested fallback arrangements and clear accountability between the entity and its providers.
Collective resilience	• Are we contributing to industry collaboration on shared risks and dependencies? • Are legal, commercial, confidentiality or competition issues being managed in a way that enables practical collaboration on shared risks? *Focus first on shared dependencies and disruption scenarios where one weak link could affect customers, markets or confidence across the system.*	Participation in information-sharing forums, exercises, sector playbooks and coordinated assurance activities.

These questions may be complemented by the material from ASD's Frontier AI Cyber Threat Considerations for Boards of Directors