Regulatory Spotlight on AI Risk Management

ASIC and APRA's Letters to Industry

In May 2026, APRA and ASIC issued letters to industry outlining their expectations for the governance, oversight and management of Artificial Intelligence (AI). The communications reflect the increasing regulatory focus on AI adoption across financial services and the associated risks and opportunities.

The letters arrive at a time of rapid AI adoption, increasing reliance on third-party technology providers and heightened cyber security concerns. Together they provide a clear indication of regulatory priorities, with APRA focusing on governance and risk management, and ASIC highlighting the evolving cyber threat environment and the impact of AI on cyber resilience. The scale of AI understanding and adoption varies across the industry however the underlying message from the regulators remains consistent.

The regulators suggest that applying the traditional risk management methods to AI will provide a foundation for managing the complexities of AI risk. However, there is an expectation that existing approaches will need to be reviewed and tested on a more regular basis to adapt to the evolving AI risk landscape.

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

What the regulators are seeing

APRA and ASIC approached AI adoption and associated risks from different perspectives: APRA focused more prominently on governance, accountability and risk management practices, while ASIC emphasised the growing cyber security implications of AI and the increasing sophistication of threat actors leveraging the technology. Several common themes emerged across both regulators.

Cyber Security and Operational Resilience

AI is changing the cyber threat landscape, giving threat actors access to increasingly sophisticated and scalable capabilities. Organisations are simultaneously embedding AI into critical business processes, increasing reliance on technology, data and third-party providers.

ASIC's communication highlights the growing cyber implications of AI adoption, while APRA reinforces the importance of maintaining robust operational resilience and risk management practices.

> "Small weaknesses can have serious, cascading consequences." – ASIC

As AI becomes more deeply embedded in business operations, organisations should assess whether existing cyber security, resilience, incident response, and crisis management capabilities remain fit for purpose in an environment where AI can both introduce and heighten cyber threats.

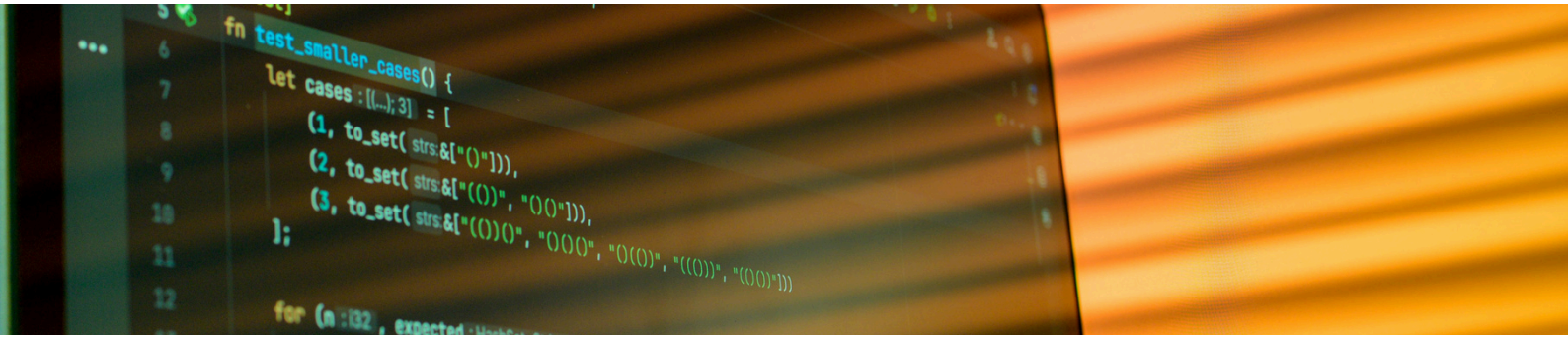
Governance and Accountability

Traditional governance models are largely designed for technology that behaves predictably. AI introduces new challenges around transparency, accountability, testing and ongoing oversight.

APRA reinforces the need for governance frameworks that support effective oversight across the AI lifecycle. Visibility of AI use cases is becoming increasingly important, particularly where AI is influencing customer outcomes, operational decisions or risk management activities.

Data governance also remains a foundational component of effective AI governance. Understanding data quality, lineage, ownership and usage is critical to maintaining confidence in AI-enabled outcomes.

Organisations should consider whether existing governance processes, approval pathways and accountability models remain fit for purpose where AI is influencing operational, risk or customer decisions.



Enterprise Risk Management

AI introduces new dimensions to existing risk categories, including operational, compliance, conduct, model and technology risk. For many organisations, the challenge is not whether existing risk frameworks apply to AI but whether they appropriately capture the speed, scale and interconnected nature of AI risks and decisions.

Both APRA and ASIC highlight the importance of identifying, assessing and monitoring AI risks within existing risk management frameworks. Organisations should also assess whether existing risk taxonomies, controls frameworks and assurance activities appropriately capture AI risks and emerging use cases.

Beyond the traditional risk management framework lens, there is heightened focus on the capability of risk functions and how well equipped risk professionals are to use and manage AI risks within their roles. As organisations mature their use of AI-enabled tools, risk professionals will need to adapt how they perform traditional activities such as incident analysis, controls testing and governance reporting. The increasing adoption of Governance, Risk and Compliance (GRC) platforms with embedded AI capabilities is creating opportunities to automate elements of these activities, allowing risk teams to focus more on analysis, challenge and strategic decision support.

Dependencies and Third Party Risk

The AI ecosystem is increasingly concentrated among a relatively small number of technology providers, models and data sources. As organisations expand their use of AI, dependency on external providers becomes a more significant risk consideration.

Understanding third-party arrangements, concentration risk, service resilience and data dependencies will be critical to maintaining effective risk management and operational resilience. This is already a key focus for the industry through the implementation and ongoing enforcement of APRA's CPS 230 Operational Risk Management Standard which places greater emphasis on third parties and material service providers.

> "Few entities had demonstrated robust contingency planning or tested exit and substitution strategies for critical AI providers". – APRA

As reliance on a small number of AI providers increases, organisations should assess whether existing third-party risk frameworks adequately address AI-specific considerations such as model reliance, concentration risk, substitution capability and data dependency. As with other critical service providers, understanding resilience, contingency arrangements and the potential impact of provider disruption will be increasingly important.

Key Consideration

The most effective organisations are not creating separate AI risk frameworks. Instead, they are adapting existing governance, risk and assurance frameworks to account for the unique characteristics of AI-enabled decision making.

Conclusion

For many organisations, the challenge is no longer whether AI will be adopted but whether governance, risk management and resilience practices are evolving quickly enough to keep pace. APRA and ASIC's communications suggest boards, executives and risk leaders should focus on understanding where AI is being used, ensuring accountability is clearly defined, assessing third-party dependencies and validating whether existing control frameworks remain fit for purpose in an AI-enabled environment.

Organisations should take this opportunity to evaluate their AI governance arrangements, confirm accountability is operating effectively, and assess how third-party AI dependencies are understood and being governed. Early action will place organisations in a stronger position to meet evolving regulatory expectations while capturing the benefits of AI-enabled innovation.

Our Authors

Poppy Fassos
Partner

With almost 30 years' experience, Poppy is a C-level executive with success in delivering and supporting some of the largest enterprise transformations in corporate Australia, building fit-for-purpose risk and compliance capabilities at an enterprise level, for Financial Services and Critical Infrastructure. Poppy offers experience in taking organisations on the full lifecycle of building and delivering risk and compliance capability and transformation through process and cultural change to enable business objectives and the right risk outcomes.

Rebecca Casey
Senior Manager

Rebecca is an operational risk professional with experience across payments, banking and advisory environments in Australia and the UK. She has supported regulatory remediation and risk transformation programs, with a focus on controls uplift, assurance and resilience. Rebecca has worked with financial services clients to strengthen control environments, including leading risk profiling activities, assessing risks and controls, and embedding first line ownership of risk. She has also delivered stakeholder-facing materials to support implementation of regulatory and internal requirements across business and risk functions.

View all services and case studies

Amstelveen

Email info@amstelveen.com

Website www.amstelveen.com

LinkedIn www.linkedin.com/company/amstelveen-pty-ltd