Scaling AI risk management and governance

What APRA-regulated entities need to scale AI safely and confidently

AI is becoming embedded in core processes and decisions, with competitive advantage increasingly determined by how safely and effectively organisations scale it.

APRA's industry letter [1] makes it clear that governance, risk management, resilience and assurance practices are not yet keeping pace with adoption. There may also be real consequences with stronger supervisory action and, where appropriate, enforcement pursued by APRA.

For APRA-regulated entities, the challenge is no longer whether to adopt AI, but how to scale it with trusted control across governance, cyber, data, supplier risk and operational resilience.

Frontier and agentic AI model (e.g., Anthropic Mythos) capabilities further reinforce the need for a step change in cyber security practices in an increasingly dynamic threat environment[2].

PwC's view is that this requires more than a governance overlay: it calls for an 'AI-native operating model'[3] where AI is built into everyday work, decisions, and processes with clearer accountability, continuous assurance and stronger control of third-party and agentic risks.

It means redesigning how people, technology, controls, and governance work together so AI can be used safely, efficiently, and at scale.

What APRA-regulated entities should act on now

01 Boards maintain sufficient **AI literacy** to set direction, challenge management and oversee AI-related risks

02 AI strategy aligned to **risk appetite** and tolerance, with clear monitoring, reporting and escalation triggers.

03 Maintain **visibility** over all AI tools, use cases and dependencies to assess where AI is used and what risks it creates.

04 Establish end-to-end **AI lifecycle governance**, from strategy and design through to monitoring and decommissioning.

05 Operationalise **controls** across key risk domains, including cyber, third-party, data integrity and privacy.

06 Understand the full AI **supply chain**, including third- and fourth-party dependencies to manage concentration risk.

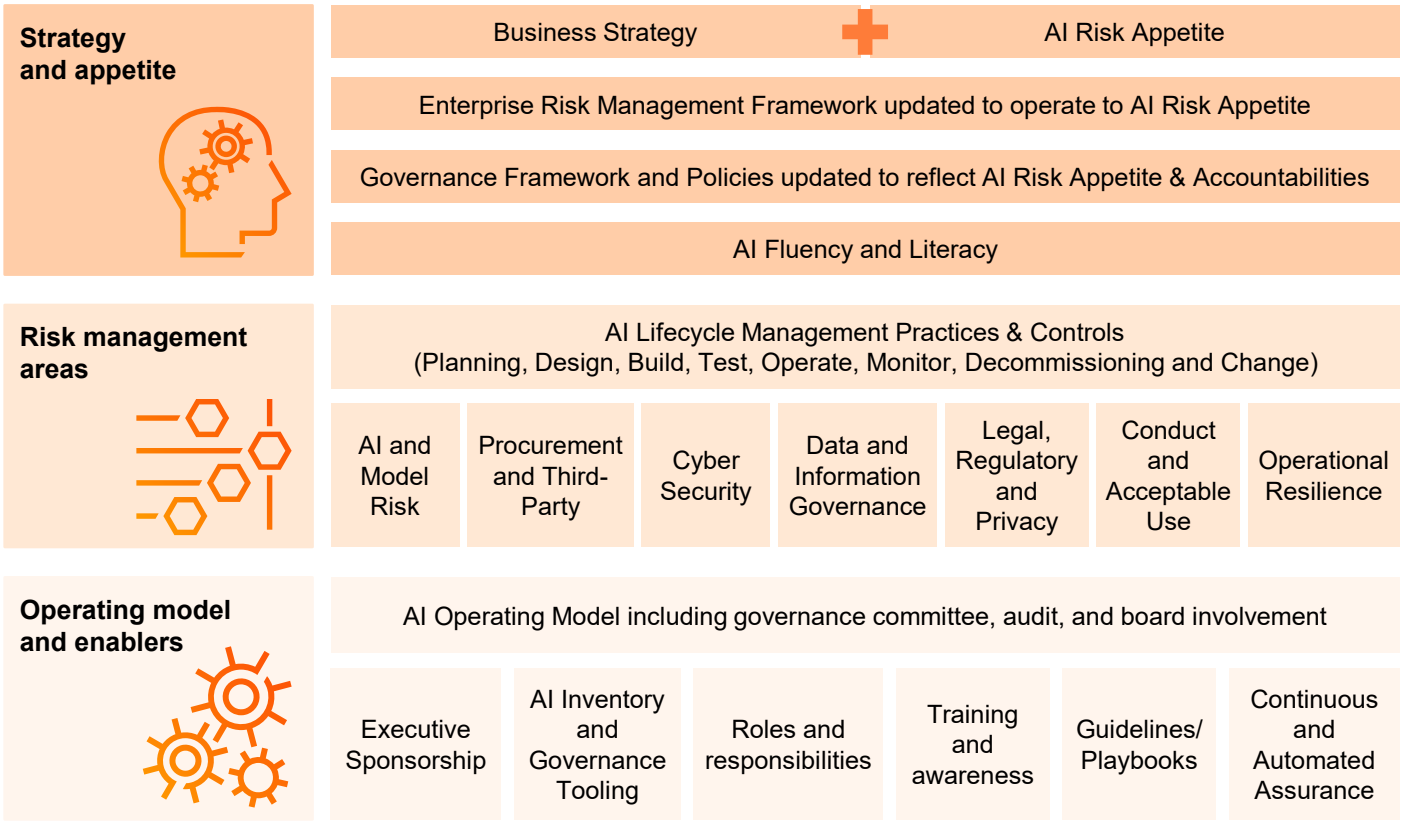
07 Strengthen **operational resilience** where AI supports critical business processes, including credible fallback arrangements.

08 Move from traditional to **continuous assurance**, integrated and technically enabled assurance.

1 apra.gov.au/apra-letter-to-industry-on-artificial-intelligence-ai
2 pwc.com.au/pdf/annual-threat-dynamics-2026.pdf
3 pwc.com.au/services/artificial-intelligence/the-ai-native-enterprise

Implications for APRA-regulated entities

Organisations need to evolve and adapt their existing enterprise-wide frameworks and practices to oversee AI and address associated risks, aligning with their risk tolerance and regulatory requirements. The PwC framework shown below highlights the essential elements needed to effectively balance AI risks and value generation on a large scale, in accordance with APRA's standards.



Practical steps to scale AI with trust and control

To scale AI safely and sustainably, regulated entities need an enterprise-wide approach that strengthens governance, control effectiveness and assurance as AI becomes embedded in core business processes. This requires clear strategic direction, alignment to risk appetite, and the deliberate redesign of controls and operating model arrangements where AI introduces new or elevated risk.

1. Build and maintain Board-level AI literacy to set strategic direction, align AI use to risk appetite and tolerance, and provide effective challenge and oversight of AI-related risks.
2. Maintain a risk-based and current inventory of AI use cases and systems, including AI deployed outside formal governance or control processes, with classification by criticality, autonomy and dependency.
3. Define, embed and test minimum control expectations across key risk domains (e.g., cyber security, data governance, third-party risk, conduct, model risk and operational resilience) proportionate to AI criticality and risk appetite.
4. Strengthen operational resilience where AI supports critical business processes, with credible fallback arrangements, substitution options and clear recovery playbooks to ensure continuity if AI degrades, fails or is withdrawn.
5. Adopt continuous, technology-enabled assurance to validate AI control effectiveness on an ongoing basis, including third-party controls, supported by monitoring, telemetry and reporting that enables timely management and Board oversight.

Contact us

Jon Benson | Partner
jon.benson@au.pwc.com

Nicola Costello | Partner
nicola.costello@au.pwc.com

Pia Chakravarti | Partner
pia.chakravarti@au.pwc.com

Bevan Lim | Partner
bevan.lim@au.pwc.com