Scaling AI risk management and governance

What organisations 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 guidance[1] is a useful reference point beyond financial services: it reinforces good-practice expectations that governance, risk management, resilience and assurance should keep pace with real-world adoption.

For non-APRA regulated entities, the challenge is to scale AI with trusted control across governance, cyber security, data quality, privacy, 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].

The Australian Government's Voluntary AI Safety Standard[3] (VAISS) reinforces these priorities through guardrails for accountability, risk management, data governance, testing and monitoring, human overview, transparency and contestability across the AI supply chain.

PwC's view is that an 'AI-native operating model'[4] is needed so AI is built into everyday work with clearer accountability, continuous assurance and stronger control of third-party and agentic risks.

What organisations should act on now

01 Boards and executives maintain **AI literacy** to set direction and oversee risks.

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

03 Maintain an **inventory** of AI tools, use cases and dependencies to understand where AI is used and risks arise .

04 End-to-end **AI lifecycle governance** from design to deployment, monitoring, change and retirement.

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

06 Manage the AI **supply chain**, including 3rd/4th parties, updates and concentration risk.

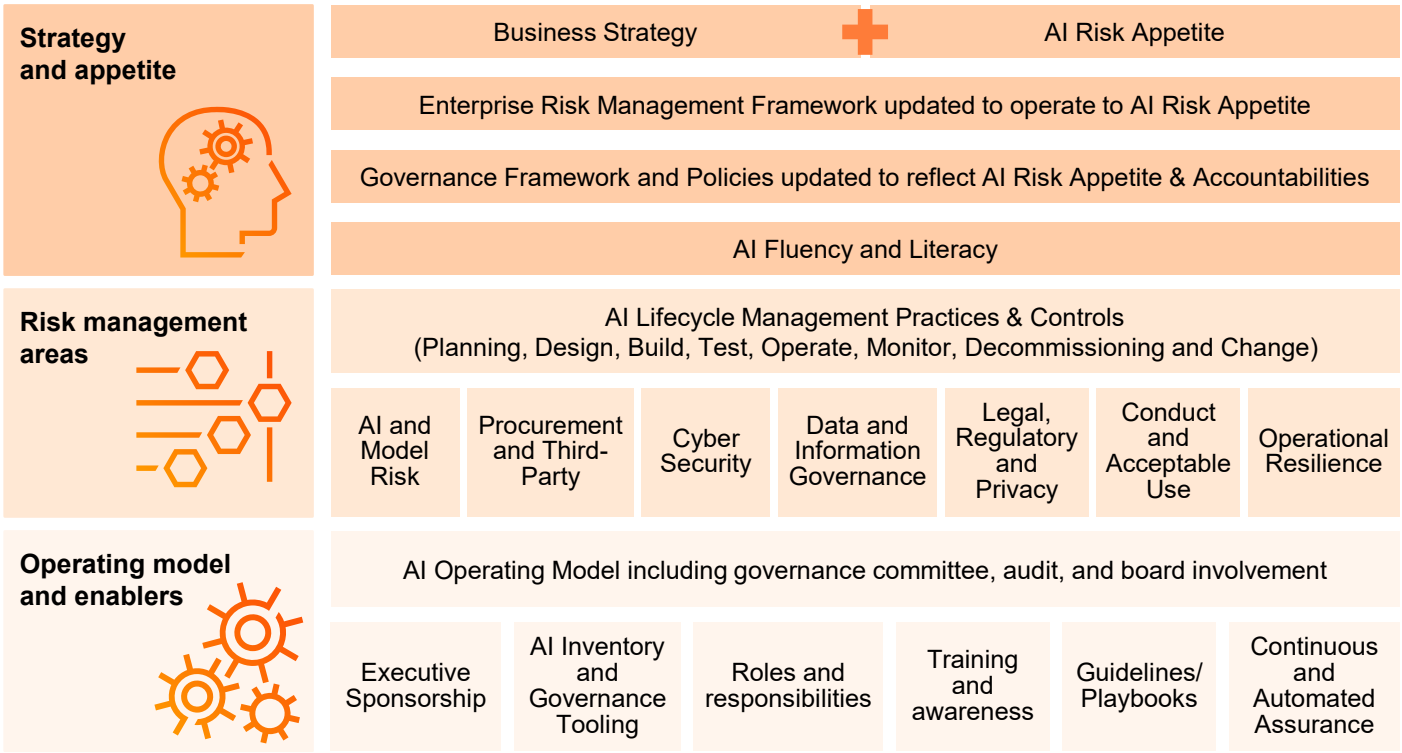
07 Strengthen **resilience** where AI supports critical processes, with credible fallback and human-in-the-loop controls .

08 Shift to **continuous assurance** using ongoing testing, monitoring and audit evidence.

1 apra.gov.au/apra-letter-to-industry-on-artificial-intelligence-ai
2 pwc.com.au/pdf/annual-threat-dynamics-2026.pdf
3 Australian Government Voluntary AI Safety Standard – industry.gov.au/publications/voluntary-ai-safety-standard
4 pwc.com.au/services/artificial-intelligence/the-ai-native-enterprise

Implications for organisations

Organisations should evolve and adapt their existing enterprise-wide frameworks and practices to oversee AI and address associated risks, aligning with their risk tolerance, stakeholder expectations and regulatory requirements. While APRA's guidance is a useful reference point beyond financial services, the PwC framework shown below highlights the essential elements needed to effectively balance AI risks and value generation on a large scale as good practice, aligned to the Australian Government's Voluntary AI Safety Standard (VAISS).



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