gadens

APRA sets clear AI expectations for the financial sector.

AI is reshaping risk across the regulated financial sector, and the regulator's guidance is clear: governance and controls must evolve – now. We set out some practical steps you can take to manage these risks below.

IT Security

Assess implications for operational reliance and business continuity

Assess the implications of relying on AI, particularly if it is intended to support critical operations. Credible fallback processes and adjustments to business continuity planning are critical to managing the risk of concentrating AI procurement with a small number of suppliers, who often exert significant power over how tools operate and can be implemented.

Identify and remediate security weaknesses

AI platforms introduce new and rapidly evolving vulnerabilities and cyber attack vectors. Deploy security controls and capabilities that address AI-specific threats including regular testing procedures to identify and remediate weaknesses.

Secure system configurations by default

Configure AI tools securely from day one – in particular where they will be used in high-risk/customer-facing settings. Disable unused features and restrict data access to only what the AI tool requires to function.

AI Governance

Establish robust, AI-specific governance frameworks

Implement governance frameworks designed specifically for AI, including identifying permitted tools and use cases, clear training to empower staff to use AI tools responsibly, and defined reporting lines.

Define accountability across the entire AI lifecycle

Assign clear ownership and accountability for every AI system – from development and deployment through to decommissioning. Beware of accountability gaps between teams to ensure nothing falls through the cracks.

Mandate meaningful human oversight

Ensure there is a 'human in the loop' to review AI-powered decisions – particularly in high-risk or customer-facing settings. Couple this with clear accountability and reviewability for outcomes.

Maintain a comprehensive AI tool inventory

Keep an up-to-date register of every AI tool in operation, recording where and how each is used. You cannot manage what you do not know.

gadens

APRA sets clear expectations for the financial sector.

AI is reshaping risk across the financial sector, and the regulator's guidance is clear: governance and controls must evolve – now. We set out some practical steps you can take to manage these risks below.

Supplier Risk & Operational Resilience

Visibility across the AI supply chain

AI services depend on multiple vendors, platforms and data sources. Organisations must understand their full AI supply chain, including material third- and fourth-party providers. Upstream risks that are not visible cannot be managed.

Transparent supplier contracts

Contracts for AI services must provide meaningful insight into how the relevant service operates, such as transparency around model updates, training, performance issues and incidents. Audit and assurance rights that enable independent risk assessment are essential to managing this.

Manage concentration risk

Where organisations rely heavily on a small number of AI providers, failures can have widespread impact. Organisations should actively manage concentration risks by planning how critical AI services could be replaced, exited or transitioned if a provider becomes unavailable or unsuitable.

Assurance & Risk Management

Coordinate AI assurance

AI risk spans cyber security, data and privacy, model performance, operational resilience and customer engagement. Assurance activities must be coordinated across all these domains as siloed approaches may leave critical gaps.

Continuous monitoring

AI systems evolve after deployment – and so do their risks. Conduct comprehensive risk and information security assessments tailored to each tool's unique capability at implementation, and on an ongoing basis.

Independent risk assessment

Internal risk and audit functions must have the technical capability, tools and access needed to independently assess AI systems and risks. This is critical to ensure AI is not implemented as a 'black box' without effective oversight.

gadens

Gadens, Australia's leading independent law firm

With over 110 partners, nearly 400 lawyers, and over 800 staff, we have offices throughout Australia in Adelaide, Brisbane, Canberra, Melbourne, Perth, and Sydney. We are well regarded for our market-leading practices in advisory, transactional and disputes work. Our client base includes multi-nationals, significant Australian corporates, private equity, and private capital instituted funds and entrepreneurs.

Key contacts

Dudley Kneller
Partner
+61 3 9252 7748
+61 438 363 443
dudley.kneller@gadens.com

Raisa Blanco
Special Counsel
+61 3 9617 8572
+61 404 047 521
raisa.blanco@gadens.com

Chris Girardi
Associate
+61 3 9612 8439
chris.girardi@gadens.com