LOVEDAY
INSURANCE SERVICES

INSIGHTS · ISSUE 04 — AUGUST 2026

AI risk management is entering the insurance conversation

Governing AI is a boardroom topic, insurers are asking more questions: what, where, who, how.

WHY IT MATTERS

AI risk, director risk: the new governance exposure

The speed of AI adoption inside organisations brings an accompanying question of governance: how are we safeguarding our business and our data in the use of AI applications?

Managing AI risk perfectly is a near-impossible exercise, requiring significant resources, significant economic spend, up-to-date AI risk management policies and processes, and following the key guidance of industry leaders and professional consultants. A gap is forming for the technology in terms of adoption versus governance - and it is increasingly being raised by boards of directors, members and shareholders, customers, insurers, regulators, even government.

> *"Increasingly, directors are expected not merely to approve AI initiatives, but to demonstrate a documented process of oversight. The question after an incident is unlikely to be whether AI was used. It will be whether the organisation can evidence what was known, what questions were asked, what testing was performed, and what governance actions followed."*
>
> Atmos, 2026

#2

artificial intelligence's rank among global business risks in 2026

#10

its rank just one year earlier - the fastest riser in the survey

Allianz Risk Barometer 2026 · 3,338 risk professionals · 97 countries

01 / REGULATORS

Regulator alarm bells

1 APRA · Australian Prudential Regulation Authority

On 30 April 2026, the Australian Prudential Regulation Authority (APRA) wrote to every bank, insurer and superannuation trustee it regulates with a blunt message: governance, risk management, assurance and operational resilience practices are not keeping pace with the scale, speed and complexity of AI adoption.

The letter followed a targeted supervisory review that found AI use accelerating across every regulated industry, moving from experimentation toward operationally embedded, customer-facing use - while governance arrangements had not matured at the same pace.

2 ASIC · Australian Securities and Investments Commission

A week later, the Australian Securities and Investments Commission (ASIC) issued its own open letter, urging licensees to urgently uplift cyber resilience and warning that frontier AI models could expose vulnerabilities at unprecedented speed, scale and sophistication.

> *"While AI adoption is continuing apace, the systems and processes required to safely govern its use aren't keeping up."*
>
> Therese McCarthy Hockey, APRA, 2026

Two of Australia's primary financial regulators, within eight days of each other, independently arrived at the same conclusion: the technology is moving faster than the controls built around it.

---

02 / UNDERWRITING

Underwriting for AI

AI risk is no longer a theoretical underwriting question. The insurance market is actively starting to build critical AI risk management data and question sets into renewal questionnaires and renewal meetings.

This is largely being seen in financial lines insurance policies focusing on the operational and governance elements of organisations: Directors & Officers Liability, Professional Indemnity, Cyber Liability and associated product classes.

AI IN INSURANCE

- **Underwriting questions**
  On proposal and renewal forms, the questions are starting to shift from a single tick-box ("Do you use AI?") to detailed due diligence on how AI is governed.
- **Terms and conditions**
  Insurers are considering AI-specific exclusions and endorsements - requiring careful policy wording review - and the question of silent AI coverage in existing policies is becoming important.
- **AI insurance products**
  Quietly growing standalone AI insurance products covering model underperformance, hallucination, and AI-related regulatory compliance failure.

AI hallucination: when an artificial intelligence model confidently generates false, misleading or entirely fabricated information that is presented as fact.

03 / DIRECTORS

Directors & Officers insurance and AI

D&O insurance exists mainly to protect individual directors and officers when they are personally sued, investigated or held accountable for decisions made in the management of the company. AI is now involved in many of those decisions - from hiring and finance to how a board itself reviews information.

When something goes wrong with AI - a biased decision, a misleading public statement, or a director missing a serious consideration because they trusted an AI-generated summary instead of reading the material - the legal responsibility still lands on the people in charge, not the tool.

CASE STUDY · STAR ENTERTAINMENT

In ASIC v Bekier [2026] FCA 196, the Federal Court found contraventions of section 180(1) of the Corporations Act 2001 (Cth) by the former CEO and General Counsel of The Star Entertainment Group, with significant penalties and disqualification periods following. The judge commented that directors cannot rely on an AI summary of board papers instead of genuinely understanding the material.

"... any use of AI should be controlled and transparent. It seems to me prudent that boards should discuss and deliberately govern any AI use by formal adoption of policies, rather than just wink at informal "shadow" use. Chairmen and company secretaries have a critical role in preserving role boundaries with management and promoting proper director engagement.

Although ethical reasoning and judgment rests with directors, not machines, AI is already changing the way in which directors receive and analyse material ..."

ASIC v Bekier (Liability Judgment) [2026] FCA 196

Regulators expect boards to understand AI well enough to properly question and oversee it, not just approve its use. The gap between using AI and actually understanding it well enough to govern it is what insurers are interested in.

In practice, that is showing up as:

- **Clear evidence of AI governance**
  Not just a policy document - who owns it.
- **Documented model testing and validation**
- **Robust oversight of third-party AI tools and vendors**
- **Safeguards against data leakage and manipulation**
- **Scenario testing that accounts for AI-driven failure, not just traditional cyber events**

04 / RESPONSE

Building a risk management response

Two frameworks are quickly becoming the practical reference points for businesses building an AI risk management approach:

NIST AI RMF

Voluntary, organised around four functions - Govern, Map, Measure and Manage - and a shared vocabulary for boards, risk and compliance teams to talk about AI risk.

ISO/IEC 42001

A certifiable management-system standard covering AI system lifecycle management, risk assessment, and third-party and supplier oversight.

APRA has also set out its expectations for AI governance in regulated entities:

- **Governance**
  Clear ownership and accountability across the AI lifecycle, an inventory of AI tools and use cases, human oversight for high-risk decisions, and staff training.
- **Supplier risk**
  Visibility over the full AI supply chain, including third-party and fourth-party dependencies, with contracts that provide transparency and auditability.
- **Assurance and monitoring**
  Recognised control frameworks and integrated risk assessment across cyber, data, privacy and model performance - with the ability to detect when an AI system's behaviour or risk profile has changed, not just when it was first approved.

APRA Letter to Industry, 2026

05 / OUTLOOK

Where this leaves Australian businesses

Australia has chosen not to regulate AI with a dedicated Act - at least for now. That does not mean the compliance bar is low. It means the bar is being set by existing law, by prudential and market regulators writing directly to industry, and increasingly by what an insurer asks before it will offer cover.

01 **Know where AI is actually being used**

A simple inventory is the starting point.

02 **Assign real ownership**

Management and the board need to be able to answer for each AI tool in use - not just IT.

03 **Introduce an AI and Digital Committee**

Oversight, challenge and strategic direction - ensuring digital and AI initiatives align with the organisation's objectives and risk appetite.

04 **Document decisions and testing**

The same principle that protects a director's position elsewhere in the business applies here.

05 **Put AI on the risk register**

Treat it as a named risk - not folded silently into "technology" or "cyber".

06 **Review the insurance program**

Assess cover against actual AI use with your broker.

CLOSING NOTE

The explanation is the point

It is not about slowing AI adoption down - it is about managing risk. Making sure the business can still explain, twelve months from now, how and why it uses the tools it does: to a regulator, an underwriter, or its own board.

That explanation is becoming as important as the technology itself.

SOURCES AND FURTHER READING

Allianz — Risk Barometer 2026
Global survey of 3,338 risk professionals in 97 countries; AI rose from #10 to #2.

APRA — Step-change in AI risk management and governance
Letter to industry, 30 April 2026, with findings and minimum expectations.

ASIC — 26-092MR: urgent cyber uplift as AI accelerates threats
Media release, 8 May 2026.

ASIC — Open letter to AFS licensees and market participants
The letter itself, with ASIC's specific expectations for licensees.

ASIC — 26-123MR: Star executives disqualified and penalised
Penalty and disqualification outcomes against the former CEO and General Counsel.

Enterprise Risk Magazine (IRM) — The case for AI and Digital Committees
Alexander Larsen, CFIRM, 29 July 2026 - why dedicated AI and digital committees are becoming necessary.

ASIC — "It's tough being a director"
Speech by Chair Joe Longo, AICD Governance Summit, 10 March 2026.

Federal Court — ASIC v Bekier [2026] FCA 196
Liability judgment of Lee J, including findings on directors' use of AI.

ISO — ISO/IEC 42001: AI management systems
The first certifiable international standard for an AI management system.

NIST — AI Risk Management Framework
Voluntary framework organised around Govern, Map, Measure and Manage.

Atmos — The New Frontier: AI-driven threat evolution
Presentation by Reece Corbett-Wilkins of cyber incident response firm Atmos on the AI leadership problem.

AI Risk Management — Insights · Issue 04 · August 2026.