AXIS / Technology

Practical Guidance

Adoption Outpacing Oversight

Why every organization needs an internal AI use framework.

Artificial intelligence tools such as ChatGPT, Google Gemini, and Microsoft Copilot have been adopted at an extraordinary speed across every sector. Employees use them to draft communications, summarize data, write code, or brainstorm ideas, often without realizing that the information they enter may be stored, analyzed, or repurposed by the tool provider.

Recent surveys show the stakes are high. Moody's Ratings' annual Cyber Survey found that while 73% of organizations have some restrictions on the use of proprietary data with public AI tools, nearly one in four have no rules at all. The exposure is even greater in the public sector, as less than half of local governments enforce any AI-use policies.

As Moody's cautioned, "Submitting proprietary information to public AI tools could expose sensitive data, potentially violating confidentiality agreements or internal data-handling rules." Risks range from intellectual property loss to data leakage and reputational damage.

Insurers Are Watching and Pricing Accordingly

The insurance market is already factoring this exposure into cyber and E&O underwriting. The Geneva Association recently reported that nine in ten businesses are interested in obtaining insurance for generative-AI-related risks, and two-thirds would pay up to 10% more in premiums to secure that protection.

Insurers, however, remain cautious. AI introduces "new layers of complexity" in estimating loss frequency and severity, particularly when incidents involve data misuse, misinformation, or algorithmic bias. The result is a widening gap between demand for AI coverage and clarity around what's actually insured.

That gap underscores a growing truth: organizations without internal AI governance will face tougher underwriting scrutiny, higher premiums, and potential coverage exclusions.

Why an AI Use Framework Matters

An internal AI use framework sets clear rules for how employees may and may not use AI tools. It aligns behavior with the company's security, legal, and compliance obligations.

Most importantly, it demonstrates governance to regulators, clients, and insurers.

Without it, organizations face three critical exposures:

1. **Data Leakage & Confidentiality Breach**

Sensitive corporate or client data entered into public AI tools can be retained or reused in ways the user cannot control. This can constitute a data breach even without a malicious actor.

2. **Intellectual Property & Copyright Infringement**

AI-generated text, code, and images may infringe third-party rights, while ownership of AI-assisted outputs remains legally uncertain.

3. **Reputational and Operational Risk**

Unvetted AI outputs, whether inaccurate product descriptions or biased recruitment prompts, can create public backlash, contractual disputes, and regulatory investigations.

A formal framework mitigates these risks by defining acceptable use and assigning accountability.

Core Elements of a Practical AI Use Framework

A good framework doesn't need to be complex; it needs to be clear, actionable, and consistently enforced.

Core components typically include:

2. **Purpose & Scope:** Define which AI tools are permitted, who can use them, and for what types of work.
3. **Data Classification & Confidentiality:** Prohibit inputting non-public, client, or personal data into external systems; require anonymization where possible.
4. **IP Ownership & Content Review:** Require human review of AI outputs before publication or client use; clarify ownership of materials created with AI assistance.
5. **Accuracy & Bias Controls:** Establish quality-control steps for factual accuracy, bias testing, and brand alignment.
6. **Security & Vendor Vetting:** Ensure AI vendors meet corporate security and privacy standards.
1. **Employee Training & Acknowledgement:** Make sure all staff understand the framework and confirm compliance annually.

The most effective frameworks are designed in collaboration among legal, insurance, compliance, information security, and HR, ensuring both enforceability and cultural buy-in.

From Risk Control to Strategic Advantage

Insurers are beginning to view strong AI governance as a positive underwriting factor, much like ISO 27001 or SOC 2 certifications. Companies that can demonstrate control over AI use are perceived as lower-risk and often obtain better terms and pricing on cyber, E&O, and D&O policies.

Beyond insurance, an internal AI framework supports:

1. Regulatory readiness, as emerging privacy and AI laws demand demonstrable governance;
2. Investor and client confidence, showing a mature approach to innovation;
3. Operational resilience, reducing costly mistakes or data loss from misuse.

A Risk Too Big to Ignore

As the Geneva Association noted, "Few technologies in history have spread as rapidly as Gen AI, yet its risks are complex and poorly understood." Businesses cannot wait for perfect clarity or regulation; governance must evolve alongside adoption.

Organizations that implement clear internal AI policies today will not only reduce exposure but also position themselves as trusted, responsible innovators.

Takeaway

AI is here to stay, but so is the risk. Building an internal AI use framework is no longer a compliance exercise; it's a business necessity that protects data, preserves trust, and improves insurability.

Develop a robust AI governance framework and align your controls with insurance market expectations.
Contact us for expert guidance today.

Contact Us

Chris Jones
Account Executive,
Mining & Technology
+1 (778) 788-2853
Chris.Jones@axisinsurance.ca

Clive Bird
Senior Vice President,
Mining & Technology
+1 (604) 817-8072
Clive.Bird@axisinsurance.ca

Stacey Copeland
Vice President,
Mining & Technology
+1 (604) 619-7775
Stacey.Copeland@axisinsurance.ca

Tristan Smith
Business Development Specialist,
Mining & Technology
+1 (416) 885-0671
Tristan.Smith@axisinsurance.ca

About

Axis Insurance - Safeguarding the Exceptional. Axis Insurance is your strategic advantage; we cut through the complexity of risk management enabling you to confidently embrace the opportunities of tomorrow. Our role is to provide you with the best insurance value that combines coverage, service and price. We also provide personalized, quality service that includes professional insurance advice, ongoing policy maintenance and claims support. When any issue arises regarding your insurance coverage, we are your advocate, using our professional experience to best represent your individual interest. Follow Axis on LinkedIn, X, Facebook and Instagram. Stay up to date by signing up for our newsletter here.

axisinsurance.ca
#2000 – 1055 Dunsmuir Street, Box 49264, Vancouver, B.C. V7X 1L2
1-800-690-7475