EVOLVING REGULATORY EXPECTATIONS FOR AI RISK MANAGEMENT FOR FINANCIAL INSTITUTIONS

Posted on January 20, 2026

Category: CNPupdates

As the financial sector accelerates its digital transformation—driven by Large Language Models (LLMs), Generative AI (GenAI) and more recently Agentic AI—Singapore's regulatory landscape in this emergent space has evolved from broad ethical/ governance principles to concrete supervisory expectations. This shift is underscored by the Monetary Authority of Singapore's (MAS) ongoing consultation (Paper P017 2025), which introduced the proposed Guidelines on AI Risk Management (AIRG) for Financial Institutions (FIs), and which are likely to be come into effect in the early part of 2026.

CNPLaw acts as legal advisor to a number of leading Singapore financial institutions and has been closely monitoring these developments in AI governance and risk management. Below is a concise briefing on the latest implications for risk management associated with FIs' integrated AI adoption.

1. **The new regulatory paradigm: from FEAT to AIRG**

The MAS' 2018 FEAT Principles—*Fairness*, *Ethics*, *Accountability*, and *Transparency*—remain the conceptual foundation for responsible AI use. However, MAS now seeks to operationalise these principles through express supervisory expectations codified in guidelines. From this year, FIs are expected to move beyond experimental deployments and adopt robust governance frameworks as AI becomes embedded in their core business processes.

2. **Determining applicability: the "integrated" use test**

The AIRG guidelines apply proportionately, based on the degree of AI integration in an FI's business and operations. All FIs must implement policies that at a minimum, define permissible and prohibited uses, and that mandate human review of AI outputs (so that there is no abdication of responsibility to machines). For FIs where AI is "integral" to business operations—meaning its absence would materially disrupt workflows or where it is embedded in critical systems—more comprehensive stricter policies must be implemented. We note that just as in other MAS policies, both "integrated" use and "materiality" are used to ensure regulation is not "one-size-fits-all" for all FIs. However, the AIRG definition of "integrated" AI usage relies heavily on the concept of "material dependence". AI is deemed integrated if the lack of access to the tool would disrupt workflows that the FI is materially dependent on, or if the AI is embedded in systems critical to business activities. This aligns with traditional materiality assessments that focus on business continuity and the impact on an FI's business operations.

3. **Core compliance requirements**

The AIRG contains several new obligations on FIs:

- To maintain a centralised, up-to-date inventory of all AI use cases, including model types, data sources, and risk ratings;
- To evaluate risks across impact, complexity, and reliance dimensions; and
- Where overall AI risk exposure is material, to establish a cross-functional governance committee (similar to how FIs oversee outsourcing of key processes).

4. **Managing third-party and "silent creeping" AI**

A growing concern is "silent creeping," where AI capabilities are embedded in enterprise software (e.g., customer relationship management or telephony) without explicit governance. To address this, the AIRG mandates that an FI must conduct due diligence on model provenance and training data integrity for third-party or open-source solutions that it uses. Further, an FI must have vendor agreements in place that include audit rights, performance guarantees, and mandatory notifications whenever the vendors introduce AI functionality.

5. **Security and Technical Resilience**

Emerging technical risks—such as hallucinations, prompt injection, and data poisoning—require targeted mitigants. As such the AIRG obliges FIs to implement override or "kill switch" capabilities for high-risk use cases when things go awry. FIs must continuously monitor for performance degradation in respect of AI enabled processes that may be due to evolving data patterns.

Conclusion

MAS's Consultation Paper signals a decisive move toward structured AI governance. It provides much needed clarity on supervisory expectations while allowing a reasonable transition period. We recommend that FIs should commence reviewing AI inventories, governance frameworks, and vendor/ third-party system arrangements to position themselves for compliance and resilience. Importantly, FIs should already incorporate AI-specific risks into their Enterprise Wide Risk Assessment (EWRA) and initiate materiality assessments to determine how much uplift is required in respect of their policies, procedures and processes.

For legal advice on AI risk management and governance, please contact Aaron Lee at alee@cnplaw.com