Baker McKenzie Wong & Leow.

Client Alert

October 2026

Singapore: MAS Issues Guidelines on Artificial Intelligence Risk Management

MAS sets out supervisory expectations on AI risk management for all financial institutions, including in relation to Generative AI and AI agents

In brief

On 7 October 2026, following a public consultation in November 2025, the Monetary Authority of Singapore (MAS) issued the Guidelines on Artificial Intelligence Risk Management ("**Guidelines**"). The Guidelines may be viewed here.

The Guidelines set out MAS' supervisory expectations relating to artificial intelligence (AI) risk management in financial institutions (FIs), and seek to support their responsible adoption of AI. They establish a set of high-level expectations that all FIs should adhere to as they deploy AI, including Generative AI and newer developments such as AI agents, in the following areas:

1. AI oversight by the board and senior management
2. Key AI risk management systems, policies and procedures
3. AI life cycle controls
4. AI capability and capacity

The Guidelines take effect on 7 October 2027. FIs may meet the expectations concerning areas 1 and 2 by 7 October 2027, and may meet the expectations concerning areas 3 and 4 by 7 October 2028.

If you have any questions on how this may impact your business or operations, please feel free to reach out to us.

Contents

Scope and application of the Guidelines
- Basic AI governance for lower-risk AI use

AI oversight

Key AI risk management systems, policies and procedures
- AI identification
- AI inventory
- AI risk materiality assessment

AI life cycle controls

AI capability and capacity

Transition period and next steps

Scope and application of the Guidelines

The Guidelines apply to all FIs in a proportionate manner, according to their size and risk profile, and on a group basis for locally incorporated FIs that are (i) subject to consolidated supervision by MAS or (ii) an owner of a critical information infrastructure. An FI which is part of a global group may leverage its group's AI risk management frameworks, as long as those frameworks meet the expectations set out in the Guidelines. However, local senior management remains accountable for ensuring that group frameworks, if adopted for Singapore, adequately address local considerations and regulatory requirements specific to Singapore.

For the purpose of the Guidelines, AI refers to machine-based systems or models that derive outputs through learned premises such as the data or inputs they receive. Calculators or tools whose outputs are solely based on predefined programming logic or rules would not be regarded as AI.

Basic AI governance for lower-risk AI use

An FI may apply only basic AI governance policies and procedures if the poor performance or unavailability of the AI services or tools used by the FI is unlikely to have a material adverse impact on the FI, its customers or other stakeholders. Examples include using AI to assist in drafting, proofreading or rephrasing emails to customers, or summarising documents or meeting notes for internal reference, provided that humans review and check the outputs before using them. Basic AI governance policies and procedures should minimally include:

(a) Clear accountability for AI oversight (e.g., by designating a member of senior management as responsible for AI oversight)

(b) Permitted and prohibited uses of AI (e.g., prohibitions on inputting confidential, proprietary or client information into public AI tools), together with effective human oversight

(c) Maintenance of an approved list of AI tools, and a defined process for requesting approval of new AI tools

(d) Staff education on the FI's AI-related policies

(e) Regular compliance checks

(f) Periodic and trigger-based review of whether the FI's AI use continues to meet the above criteria

Otherwise, an FI should meet the full set of expectations in the Guidelines, as summarised below.

AI oversight

The board of directors and senior management of an FI play critical roles in establishing and overseeing robust frameworks, policies and procedures to support AI risk management across the FI. They should ensure that existing risk management frameworks, policies, and practices adequately identify, assess, and address risks posed by AI, and ensure consistent and coordinated management of risks from AI use across all relevant functions. In particular:

- The board, or a committee delegated by it, is responsible for, among other things, approving the overall governance approach for AI risk management and ensuring that risks from AI use are explicitly addressed within the FI's risk appetite framework.
- Senior management is responsible for, among other things, ensuring the effective implementation of AI-related risk management frameworks that are consistent with the FI's risk appetite, establishing clear roles and responsibilities for managing risks from AI use, and establishing an internal escalation process for managing material risks and exceptions from AI use, such as AI incidents.

Key AI risk management systems, policies and procedures

An FI should ensure that its AI risk management framework encompasses key systems, policies and procedures for the identification, inventorisation, and risk materiality assessment of AI. For each of these, the FI should designate a control function which retains sufficient and independent oversight, even where the work may be carried out by relevant business or functional units.

AI identification

An FI should establish systems, policies and procedures to ensure the consistent identification of AI use across all relevant business and functional areas. Where AI is incorporated within, or used in the delivery of, services provided by material third-party service providers, the identification process should minimally cover such AI. The designated control function should be the final arbiter on whether a given use constitutes AI use. Where there are practical constraints in consistently identifying all AI use, e.g., the use of shadow AI, the FI should identify risks that arise from such constraints, and put in place mitigating measures.

AI inventory

An FI should establish and maintain an accurate inventory of AI use cases, systems or models across the FI to the extent possible or practicable, either by enhancing existing inventories or establishing a dedicated AI inventory. The AI inventory should capture key attributes at an appropriate level of granularity to enable effective governance and oversight, as well as risk management. FIs can choose to either enhance their existing inventories to include AI use cases, systems or models, or establish a dedicated AI inventory.

AI risk materiality assessment

An FI should establish an assessment methodology to evaluate the risk materiality of an AI use case based on the nature of its business and the risks arising from the systems and models used. The assessment should take into account both the inherent risk materiality before risk management controls are applied, and the residual risk materiality after such controls are applied. The assessment should minimally cover the following risk dimensions:

- **Impact:** The potential consequences of a failure, malfunction, or poor performance of the AI on the FI and its customers or other stakeholders
- **Complexity:** Arising from the nature of the AI technology used, the novelty of its application, the data it uses, or the explainability of its outputs

- **Reliance:** The level of reliance on AI for the associated decision or output, including the extent of autonomy granted to the AI and the degree of human involvement or oversight

AI life cycle controls

An FI should plan for and implement robust controls covering the entire life cycle of an AI use case, system or model, in a manner proportionate to its assessed risk materiality of the particular use case. For an AI use case assessed as high risk, an FI should develop and implement contingency plans outlining fallback options, such as alternative systems or manual processes. The Guidelines set out controls in the following areas:

- **Data management:** Data used across the AI life cycle should be fit for purpose and representative, of high quality, and subject to robust data governance.
- **Transparency and explainability:** The degree of transparency and explainability required should reflect the context and nature of the AI use case and its assessed risk materiality.
- **Fairness:** An FI should define what it considers "fair" outcomes and have appropriate controls to identify and mitigate harmful biases and discriminatory outcomes across the AI life cycle.
- **Human oversight:** An FI should put in place and regularly review controls to ensure appropriate human oversight over an AI use case, system or model across its life cycle, taking into account automation bias and decision fatigue.
- **Third-party AI management:** The FI retains primary accountability for its use of third-party AI. The FI should ensure that onboarding, development and deployment controls are adequate for the risk materiality of the use case involving third-party AI. For instance, contractual agreements with third-party providers should give the FI a risk-appropriate degree of visibility over the introduction of AI and subsequent updates or changes. Where the residual risk materiality cannot be kept within the FI's risk appetite, the FI should consider limiting or suspending the third-party AI service, or replacing the provider.
- **Selection:** When selecting AI systems, models or features to use, an FI should consider the objectives and risks of the AI use case.
- **Evaluation and testing:** Each system or model should be evaluated and tested to meet an appropriate level of reliability and safety before deployment.
- **Technology and cybersecurity risks:** The AI system should be secure, well-governed, and supported by appropriate controls to manage technology and cybersecurity risks.
- **Reproducibility and auditability:** The AI development process should be documented in sufficient detail for an independent party to understand and potentially replicate the implementation of the AI system or model and its evaluation and testing process.
- **Pre-deployment reviews:** AI use cases should be reviewed by parties not involved in their development, and those use-cases that are assessed as having high risk materiality should undergo formal independent validation before deployment.
- **Post-Deployment Monitoring and Review:** An FI should implement comprehensive and robust controls for the ongoing monitoring of all deployed AI (including third-party AI). AI use cases assessed as having high risk materiality should be subject to re-validations by independent parties, on a more frequent and rigorous basis.
- **Change management:** An FI should implement robust controls for managing changes to deployed AI, as well as for the eventual retirement or decommissioning of AI.

AI capability and capacity

An FI should determine and ensure the necessary competence and proper conduct of personnel involved in developing, deploying and using AI, and ensure that its technology infrastructure is adequate for the AI use cases, systems or models it wants to implement.

Transition period and next steps

The Guidelines take effect on 7 October 2027. FIs may meet the expectations on AI oversight and key AI risk management systems, policies and procedures from 7 October 2027, and those on AI life cycle controls and AI capability and capacity by 7 October 2028. MAS has also indicated that it intends to consult the industry in 2027 on further guidance on agentic AI. As AI adoption and its associated risks will continue to evolve alongside advancements in AI technologies, MAS may update or augment the Guidelines where needed.

FIs should take stock of their current and planned AI use, including AI embedded in third-party services, assess whether basic AI governance policies and procedures would suffice, and map their existing frameworks against the applicable expectations to plan for compliance within the above timelines.

Contact us



Stephanie Magnus
Principal
stephanie.magnus
@bakermckenzie.com



Eunice Tan
Principal
eunice.tan
@bakermckenzie.com



Darren Yang
Local Principal
darren.yang
@bakermckenzie.com



Lee Zhe Xu
Local Principal
zhexu.lee
@bakermckenzie.com

© 2026 Baker & McKenzie.Wong & Leow. All rights reserved. Baker & McKenzie.Wong & Leow is incorporated with limited liability and is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "principal" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.