Factsheet- Model AI Governance Framework for Agentic AI

What is the Model AI Governance Framework for Agentic AI?

The Model AI Governance Framework (MGF) for Agentic AI gives organisations a structured overview of the risks of agentic AI and emerging best practices in managing these risks. If risks are properly managed, organisations can adopt agentic AI with greater confidence.

Who is the MGF for Agentic AI for?

The MGF for Agentic AI is targeted at organisations looking to deploy agentic AI, whether by developing AI agents in-house or using third-party agentic solutions.

What does the MGF for Agentic AI cover?

The MGF for Agentic AI outlines key considerations for organisations in four areas across the agentic AI lifecycle:

1) Assess and bound the risks upfront
    - Know the risks – determine suitable use cases for agent deployment by carrying out a risk assessment, considering agentic-specific factors such as the agents' access to sensitive data and level of autonomy
    - Bound the risks – limit the scope of impact of such risks through early design choices, such as setting limits on agent autonomy, tools and data access
2) Make humans meaningfully accountable
    - Clear allocation of responsibility across multiple parties in agent lifecycle
    - Design effective human oversight to guard against automation bias e.g. trigger human approvals at significant checkpoints, and regularly audit the effectiveness of such human approvals
    - Emphasise adaptive governance by setting up the organisation to understand new developments and update approaches as technology evolves
3) Implement technical controls and processes
    - During design and development – design and use technical controls to mitigate risks in new agentic components such as planning, tools, and protocols
    - Pre-deployment – test agents for baseline safety and security
    - During and post-deployment – gradually roll out agents by limiting to certain users or features first, complemented by continuous monitoring and testing

4) Enable end-user responsibility

- Transparency – inform users of when and how agents are used
- User education – train users on how to use agents responsibly and oversee agents effectively, while ensuring that users retain foundational skills

What organisations have to say about the MGF for Agentic AI

David Sully, CEO/Co-Founder, Advai

"Agentic AI is arriving fast, and strong technical assurance will be critical to deploying it safely and securely. IMDA's Model AI Governance Framework for Agentic AI is therefore timely. Singapore continues to set the pace on AI assurance, and I'm looking forward to Advai applying this framework in practice."

Elsie Tan, Country Manager, Worldwide Public Sector, Singapore, Amazon Web Services

"Agentic AI systems will make decisions with real-world consequences. We need concrete mechanisms for visibility, containment, and alignment built into infrastructure, along with human judgment to use them wisely. Singapore's Model AI Governance Framework is a step in the right direction."

Serene Sia, Country Director, Malaysia and Singapore, Google Cloud

"Building trust in agentic AI is an ongoing, shared responsibility, and IMDA's framework is a constructive first step. Having pioneered open standards like the Agent2Agent Protocol (A2A) and Agent Payments Protocol (AP2), Google has been playing a key role in establishing the foundation for interoperable and secure multi-agent systems. We remain committed to responsible innovation and look forward to contributing best practices as this technology advances further."

Dr. Komes Chandavimol, Principal AI Evangelist, KASIKORN Business-Technology Group

"At KBTG (KASIKORN Business-Technology Group), the technology and innovation arm of KASIKORNBANK (KBank), we have already begun deploying AI agents across the bank and have a strong pipeline of additional agents ahead. As we move toward deployment at scale, we are

strengthening our agentic AI governance. The Model Governance Framework for Agentic AI (MGF) is a timely and practical document that will help guide this journey."

Ying Shao Wei, Chief Scientist, NCS

"IMDA's Model AI Governance Framework for Agentic AI provides NCS and the industry with a practical, Singapore-anchored approach to deploying Agentic AI with confidence. It enables organisations to move from pilots to production with confidence, ensuring risk management keeps pace with progress. This aligns with NCS' core approach: identify the right problems to be solved, assess risks, and test—then move to production only with proper safeguards and observability in place."

April Chin, Co-Chief Executive Officer, Resaro

"As the first authoritative resource addressing the specific risks of agentic AI, the MGF fills a critical gap in policy guidance for agentic AI. The framework establishes critical foundations for AI agent assurance. For example, it helps organisations define agent boundaries, identify risks, and implement mitigations such as agentic guardrails.

By providing organisations the agentic assurance structure, the framework creates clear "hooks" for testing. For example, third-party testers such as Resaro can stress test agentic guardrails or boundaries to ensure the agents behave as intended in realistic deployment contexts.

This lays important groundwork for assurance providers like Resaro, because we can build on the framework to design practical testing strategies for agentic AI around key risks and technical controls."

Nina Alag Suri, Founder and CEO, X0PA AI

"Agentic AI marks a fundamental shift in how organisations make decisions and execute actions. This framework matters strategically because it positions governance not as a constraint, but as an enabler of scale—defining where autonomy is appropriate, where human judgment must prevail, and how accountability can be embedded as agents become integral to core operations."