



Agentic AI & Security Governance Blueprint



What it is:

An application to prioritise security controls for agentic AI systems

CISOs



AI Governance & Compliance Leaders



Technology Risk Leaders



Why it matters

As organisations expand AI adoption and explore frontier AI, autonomous agents introduce new risks across data, identities, tools and interconnected systems. Security teams also face growing pressure to use AI to augment threat analysis and control prioritisation. Understanding each agent's capabilities, autonomy and operating context enables organisations to apply proportionate controls, strengthen oversight and scale adoption with greater confidence.

Identify agentic AI threats and prioritise controls based on system autonomy, architecture and risk context.

What it does: Prioritise the right controls for agentic AI

Understand AI operating context and autonomy level

Establish an accurate risk baseline.

Map threats across the MAESTRO 7-layer model

Identify where agentic risks emerge.

Prioritise security controls

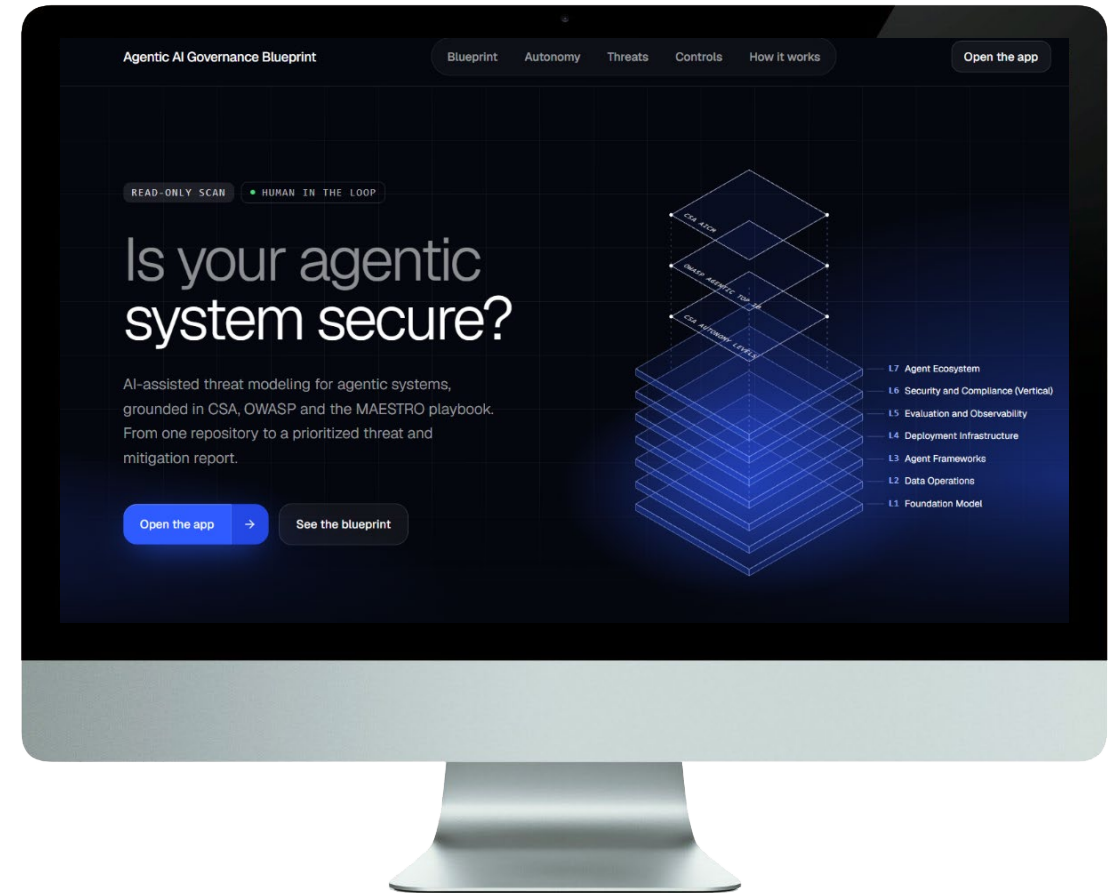
Focus remediation on the most material exposures.

Guide control implementation

Operationalise security and compliance requirements consistently.

Benefits

- Stronger alignment between security and compliance
- Consistent governance across AI deployments
- Clear control implementation priorities
- Accelerates secure enterprise AI adoption



How it works: Demo

Input

Define the business context, system architecture, AI capabilities and autonomy level to establish risk and governance requirements.

Action

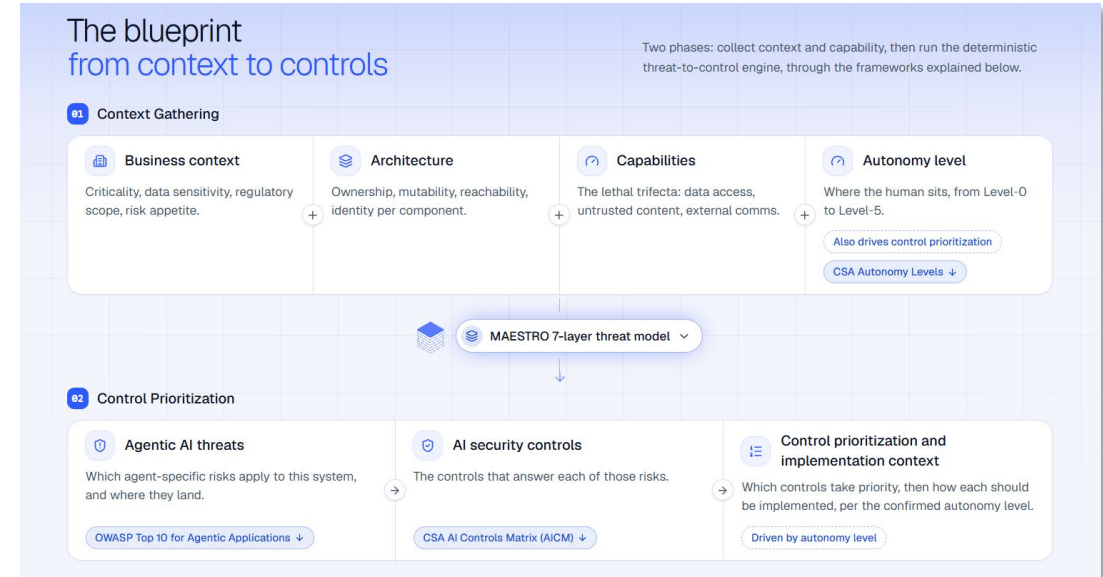
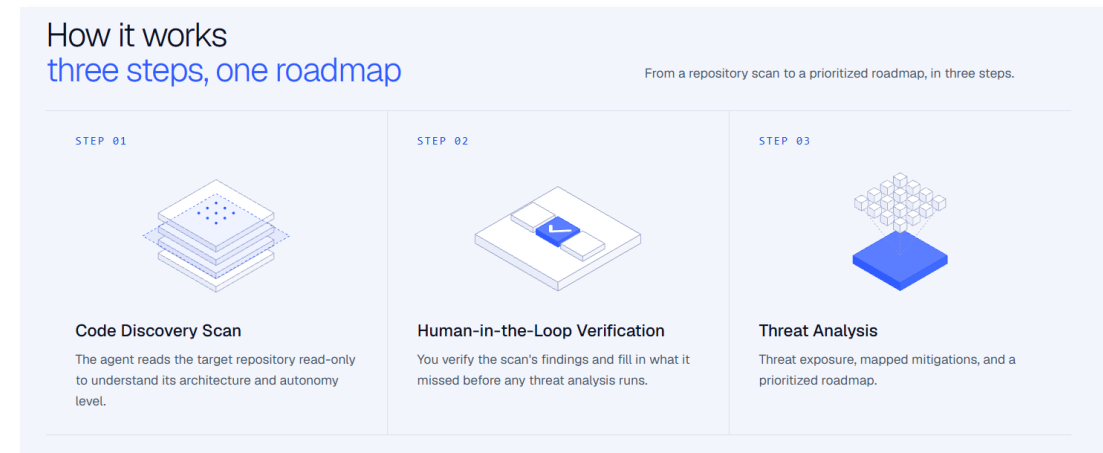
Conduct a code discovery scan, validate findings through human-in-the-loop review, and assess risks across the MAESTRO 7-layer model to align controls and prioritise implementation actions.

Output

A prioritised view of agentic AI threats, recommended controls and implementation considerations.

Impact

Accelerate secure AI adoption through risk-informed governance and deployment decisions.



Build confidence in enterprise agentic AI

Discover how AI context, threats and controls support informed deployment decisions.

Consider a discussion if your organisation is:

- Adopting agentic or autonomous AI capabilities
- Scaling AI across business-critical operations
- Establishing governance for frontier AI initiatives

Request a consultation to turn AI ambition into secure and trusted adoption.



Jianshu Weng

Director, Cyber,
KPMG in Singapore

gavankingdon@kpmg.com.sg



KPMG Services Pte. Ltd.

© 2026 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

General disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Document Classification: KPMG Public