



Scaling your AI & NHI Governance



What it is:

A solution to govern AI agents and non-human identities

SecOps & Identity Teams



IT Operations & Engineering Teams



Risk, Compliance, & Governance Teams



Why it matters

AI agents can access data, invoke tools and execute actions as privileged non-human identities.

Separate AI and identity controls can leave ownership, access and activity fragmented. Converging both control domains provides lifecycle governance, contextual access, continuous monitoring and audit evidence to support safe, traceable adoption.

Govern AI agents, non-human identities and access ecosystems through integrated governance, automation and continuous assurance.

What it does:

Establish control across the AI identity lifecycle

Discover AI agents, machine identities and access relationships

Establish a trusted inventory.

Modernise identity platforms and data foundations

Support scalable AI adoption.

Govern agent access and execution privileges

Maintain accountability and least privilege.

Automate IAM operations and continuously monitor controls

Improve efficiency and reduce risk.

Benefits

- Faster AI governance adoption
- Improved IAM operational efficiency
- Stronger compliance and audit readiness



How it does it: Demo

Input

AI agents, non-human identities, IAM platforms, access data, operational support requests and governance requirements.

Action

The solution discovers identities and agents, modernises identity foundations, applies governance controls, automates IAM support activities and continuously monitors control performance.

Output

A unified view of AI agents, machine identities, permissions, activity, risks, support insights and control performance.

Impact

Securely scale AI adoption through greater visibility, governance oversight and continuous assurance.



Explore trusted AI identity governance

Discover how to modernise identity foundations, govern AI agents and continuously monitor controls across your growing AI ecosystem.

Consider a discussion if your organisation is:

- Scaling AI agents across enterprise operations
- Modernising identity platforms for future growth
- Strengthening governance, compliance and assurance

Speak to us on how you can bring visibility and control to AI identities.



Dhananjay Jhadav

Director, Cyber,
KPMG in Singapore

djadhav@kpmg.com.sg

KPMG's Offering: AI and Non-Human Identity Protection

The adoption of AI agents, autonomous models, and architectures based on connected tools introduces a new paradigm of non-human identities with the ability to access, reason, and execute on corporate systems. AI agents require governance, contextual controls and continuous monitoring to support safe, traceable use and least-privilege access.

Description

- **AI Identity Discovery and Inventory:** Automatic identification of agents, models, MCP Servers, tools, and non-human accounts deployed in cloud environments, AI platforms, and corporate ecosystems.
- **Lifecycle governance:** Management of registration, modification, review, and retirement of non-human identities, including credential rotation, privilege review, and dependency control.
- **Contextual control:** Application of dynamic policies based on context, criticality, data sensitivity, expected behavior and level of operational confidence of the agent.
- **Authority-in-execution:** Controlled delegation of execution capabilities for AI agents (through validation and certification processes) limiting critical actions through human approval, sandboxing, and functional segregation.
- **Operational monitoring and traceability:** Continuous supervision of accesses, tool calls, prompts, actions executed and communications between agents and corporate systems.

Benefits

- ✓ Reduction of the risk associated with autonomous agents and unsupervised access
- ✓ Granular control over execution capabilities and use of corporate tools
- ✓ Greater traceability and auditability on actions executed by non-human identities
- ✓ Protection against abuse of privileges, prompt injection and tool hijacking
- ✓ Alignment with Zero Trust principles as well as market standards such as AI Act, NIST AI RMF and ISO 42001

Our approach

We apply a non-human identity protection model based on Zero Trust, Identity Threat Detection & Response (ITDR) and contextual authorisation principles, specifically adapted to AI ecosystems and autonomous agent architectures. Our approach combines capabilities of:

- **AI Agent Governance and Control:** Centralised management of autonomous identities, trust relationships, effective privileges, and control of connected tools.
- **Dynamic Contextual Authorisation:** Real-time assessment of: identity, requested action, resource sensitivity, contextual risk, expected behavior, and operational criticality.
- **Tool Protection and MCP Servers:** Enforce policies on: read/write, execute actions, access APIs, invocation of tools, and communication between agents.
- **Behavior and anomaly monitoring:** Detection of: abuse of privileges, unauthorised escalations, anomalous access, tool hijacking, malicious automations and operational deviations.
- **Observability and complete auditing:** Traceability of: prompts, decisions, tool invocations, actions executed, permissions used and complete flow of interaction between agents and systems.



KPMG's Approach

1

PHASE 1— Strategic Assessment and Definition



Results and objectives achieved:

- Complete visibility into the current state of AI adoption in the company and its main risks
- Baseline of maturity and security priorities
- Map of gaps and initiatives by impact
- Roadmap by phases: quick wins, short and medium term



Assets / Deliverables

- Inventory of models, datasets, pipelines, apps, and prompts
- Maturity assessment: score, findings and recommendations
- Current technology landscape and coverage assessment
- Risk analysis: abuse, leakage, prompt injection
- High-level target architecture

Key output Prioritised backlog of initiatives

8 weeks

2

PHASE 2— Design and Implementation of Production Capabilities



Results and objectives achieved:

- Deployed and operational capabilities
- Automated controls and enforced governance
- Basic detection and response capabilities in place
- Recurring reporting models and procedures for management and technical teams



Assets / Deliverables

- Configuring Security and Monitoring Tools
- Integrations with SIEM/SOAR, MLOps, IAM, and logging
- Control automation: policy-as-code and guardrails
- Playbooks of incidents, severity, RACI and SLAs

Key output KPIs/KRIs dashboards

Key output Controls operationalised

4-6 months

3

PHASE 3— Operation and Continuous Evaluation



Results and objectives achieved:

- Continuous operation (tuning, hardening and continuous improvement)
- Proactive management of the company's risk and exposure level
- Evolving controls in the face of new threats
- Constantly evolving operational governance



Assets / Deliverables

- Managed Service Model: Scope, SLAs, and Roles
- Continuous monitoring and incident response
- Triage, containment and post-mortem
- Periodic review of controls monthly/quarterly
- Executive reports with trends, gaps, and actions

Key output Continuous improvement plan in place

Ongoing

Secure AI adoption requires turning strategy into operational, measurable, and sustainable capabilities

KPMG Accelerators

01

Migration to the cloud

Secure, structured move of identity and data workloads to the cloud.

02

IAM support agent

AI agent that resolves routine identity and access requests.

03

IAM and data lineage studio

Maps who can access which data, and how data flows across systems.

04

Continuous control monitoring dashboard

Real-time view of control health, exceptions and compliance status.

05

Agentic Fabric training

Hands-on enablement for teams to build and govern AI agents.



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