



NHI & AI Governance Maturity Model

Five levels, from Ad hoc to Optimised, for governing non-human identities and the AI agents that now use them. Assess each identity type on each platform, weight by exposure, and fix first where privilege is highest and maturity lowest.



Two dimensions

Type of identity: certificates, API keys, tokens, secrets, directory service accounts, workload identities, AI agents

Platform: public cloud, on-premises, databases, mainframe, SaaS, third-party applications

How to use the model

1

Map your maturity

Score each identity type on each platform.

2

Weight by exposure

Privilege, sensitive data, closeness to production.

3

Fix the worst first

Highest privilege, lowest maturity.

4

Reassess regularly

AI agents change fast.

What each level looks like, and how to move up

LEVEL	NON-HUMAN IDENTITIES	AI AGENTS	NEXT STEPS
1 Ad hoc Weak controls, no visibility, unmanaged and stale accounts, secrets hardcoded into source.	- No inventory of non-human identities - Credentials embedded in source code - Stale, unmanaged accounts persist	- Agents deployed without registration - Running on credentials inherited from proof-of-concept developers - Agent population unknown and ungoverned	- Build a first inventory of NHIs and AI agents - Find and remove secrets hardcoded in source code - Give every critical account and agent an owner
2 Developing Policies and standards exist on paper, a partial inventory has been built, and controls and hygiene are manual. Audits are ad hoc rather than continuous.	- Written policies and standards in place - Partial inventory - Manual controls and hygiene - Ad hoc audits	- Sanctioned agents roughly known; shadow agents invisible - Agents not separated from other NHIs in the inventory - Autonomous agents treated like batch-job service accounts	- Complete the inventory across every platform - Tie ownership to applications, not people - Deploy a secrets vault and scan pipelines for secrets - Create a mandatory agent catalogue
3 Defined Governance is formally in place, inventory and ownership are established, secrets vaulting is deployed and scanning is integrated into CI/CD pipelines.	- Formal governance framework operating - Inventory with ownership tied to applications and services - Secrets vaulting deployed - Secrets scanning in CI/CD pipelines	- Mandatory agent catalogue - Every agent registered with its scope and purpose - Joiner, mover, leaver processes extended to agents - Agents without an owner do not run	- Automate provisioning and decommissioning - Rotate secrets automatically - Switch on monitoring and orphan-agent detection
4 Managed Provisioning and decommissioning are automated, lifecycle management is in place, secrets are secured and cycled without manual intervention, and monitoring controls are operational.	- Automated provisioning and decommissioning - Lifecycle management in place - Secrets rotated without manual intervention - Monitoring controls operational	- Behaviour baselines replace static rules - Continuous detection of orphaned agents - Recertification triggered by model updates - New capabilities approved before reaching production	- Move to just-in-time, short-lived credentials - Make access policy-based and context-aware - Automate remediation of anomalies
5 Optimised Preventive controls operate by default, dynamic just-in-time credentials replace static ones, access is policy-based and context-aware, and security is integrated rather than bolted on.	- Preventive controls on by default - Just-in-time credentials replace static secrets - Policy-based, context-aware access - Anomalies detected and remediated automatically	- Authorisation checked at the moment of action - Credentials scoped to a single task - Trust-chain policy enforced at every agent handoff - Drift detected and credentials revoked automatically	- Keep policies and baselines tuned as agents change - Test revocation and kill switches regularly - Reassess as new identity types and platforms appear

Where are you today? Take the free NHI & AI Governance Maturity Assessment at nhimg.org/nhi-ai-maturity-assessment · Full model: nhimg.org/nhi-ai-governance-maturity-model