



CYBERSECURITY | MANAGED SERVICES

Managed AI Governance

Continuous visibility, governance insight and advisory for enterprise AI adoption

The governance gap is already costing you

AI adoption inside most organisations has outpaced the ability to oversee it. Staff are using tools that IT has never seen, agents are proliferating without lifecycle controls, and consumption costs are climbing without anyone tracking where the spend is going

That gap is no longer a theoretical risk. IBM's Cost of Data Breach research found that 20% of organisations have traced a breach directly to shadow AI, adding an average of £200,000 to total incident costs.¹ With EU AI Act obligations now live and high-risk system deadlines set for December 2027, the window to get ahead of this is narrowing.

£200K

average added breach cost when shadow AI is involved¹

78%

of enterprises are unprepared for EU AI Act obligations³

What Managed AI Governance does

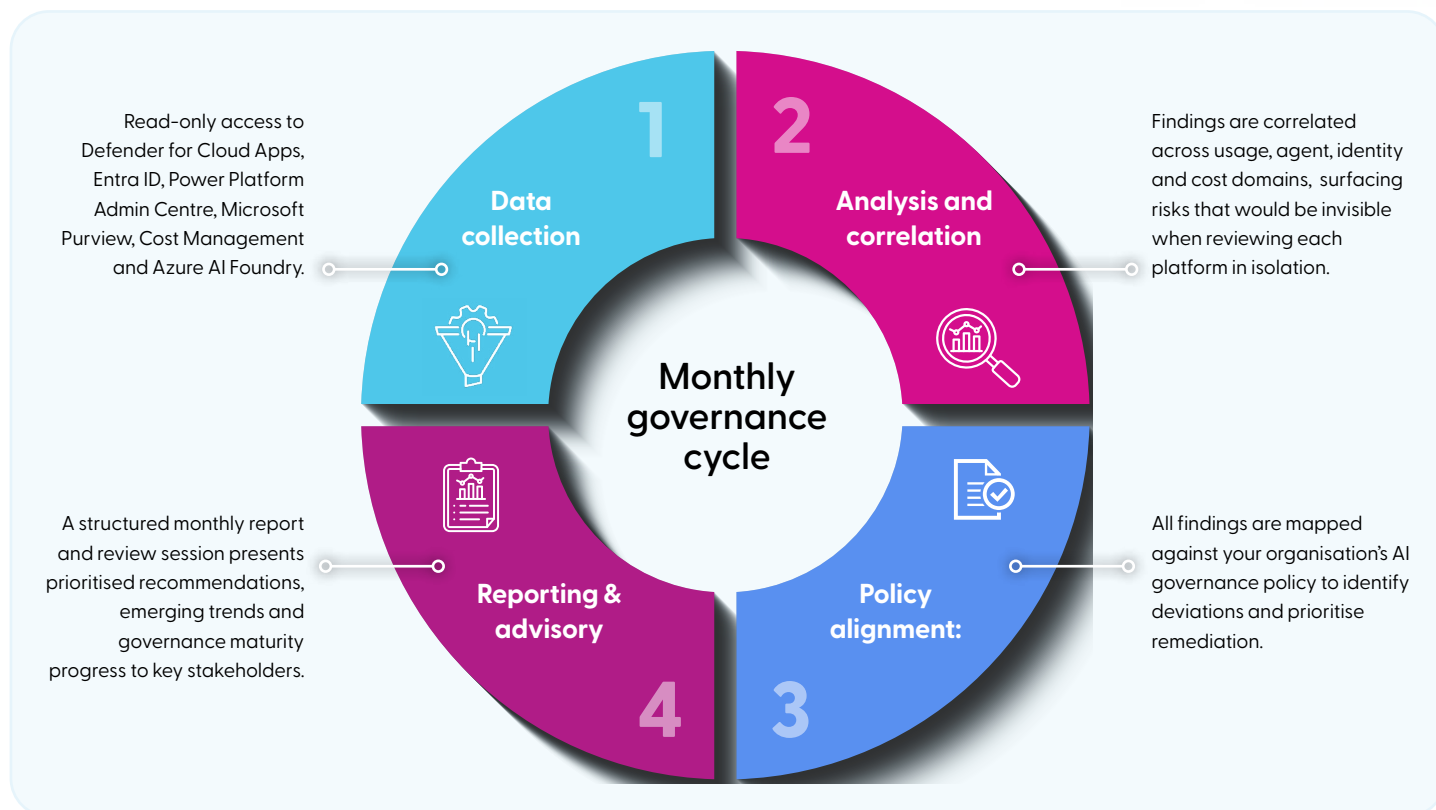
Managed AI Governance is a recurring managed service that gives organisations structured, continuous oversight of their AI estate. Rather than a one-off assessment, it operates on a monthly governance cycle, collecting data from native Microsoft telemetry, correlating findings across usage, identity and cost domains, and turning them into prioritised, policy-aligned recommendations your team can act on.

Four areas of continuous oversight

- | | |
|---|--|
| 1 AI Usage Visibility & Shadow AI Governance | Identifies every generative AI tool in use across the organization, sanctioned or otherwise. Draws on Microsoft Defender for Cloud Apps telemetry to surface adoption patterns, high-usage departments and data interaction volumes, without inspecting content. |
| 2 AI Agent & Automation Governance | Provides a centralised inventory of Copilot Studio agents, SharePoint agents and Power Platform integrations. Tracks lifecycle status, active, inactive, unused, and flags agent sprawl before it becomes an operational or financial liability. |
| 3 AI Identity Governance | Maps the service principals and application identities tied to AI workloads. Highlights orphaned accounts, overprivileged access configurations and deviations from least-privilege principles, the non-human identity layer that most security programmes still treat as an afterthought. |
| 4 AI Cost Trends Analysis | Tracks Copilot Studio consumption patterns and cost distribution across environments and business units. Identifies low-value workloads generating spend without delivering returns, and provides optimisation recommendations as vendors accelerate the shift to consumption-based billing. |

How the service works

The service follows a structured Plan → Build → Manage methodology. Onboarding establishes the governance framework and data access. The build phase validates connectivity to Microsoft data sources and configures the reporting foundation. From there, the service runs on a recurring monthly cadence.



Scope at-a-glance

Included in the service

- ✓ Visibility and discovery of AI usage
- ✓ Monthly governance reporting and dashboards
- ✓ Auditing and compliance evidence
- ✓ Trend analysis, benchmarking and insights
- ✓ Policy-aligned advisory and recommendations

Outside the service boundary

- Technical implementation and remediation
- Runtime policy enforcement
- Security monitoring (SOC / MXDR)
- Content inspection of AI inputs or outputs

Implementation of recommendations can be delivered separately through Insight Professional Services.

What you gain

- Full visibility into AI tool usage across the enterprise, including shadow AI
- Control over agent lifecycle and early detection of agent sprawl
- Improved identity governance and reduced access risk from non-human identities
- Optimised AI spend and consumption patterns as billing models shift
- Policy alignment with measurable, reportable governance outcomes
- Continuous insights that support responsible, scalable AI adoption

Why the timing matters

The regulatory environment has shifted from guidance to enforcement. The EU AI Act is fully applicable from 2 August 2026, with high-risk system obligations for standalone AI, including recruitment, credit scoring and biometric tools, set for 2 December 2027 following the Digital Omnibus amendments agreed in May 2026.² Fines for prohibited practices are already live at up to €35 million or 7% of global annual turnover, whichever is higher.



Organisations operating in or selling into EU markets face the same extraterritorial scope as GDPR. Meanwhile, the ICO published its first report on agentic AI in January 2026 and has confirmed active monitoring of AI deployments throughout the year. For businesses still running ungoverned tools, that monitoring represents a live enforcement risk, not a future one.

Organisations that establish governance foundations now will be better positioned to scale AI responsibly, and to demonstrate that maturity to regulators, customers and boards.

Why Insight?

Insight brings together deep Microsoft ecosystem expertise, enterprise AI governance experience and a proven managed services delivery model. The service is built on native Microsoft telemetry, Defender for Cloud Apps, Power Platform Admin Centre, Entra ID, Purview and Cost Management, so there is no additional tooling to procure or integrate.

Critically, the service maintains a clear separation between advisory and implementation. Insight provides the visibility and recommendations; your team retains decision-making authority. Where implementation support is needed, Insight Professional Services can be engaged separately.

As the leading Solutions Integrator, Insight connects governance, security and AI adoption strategies holistically – helping organisations move from fragmented oversight to a structured, scalable programme that grows with their AI estate.

Getting started

Prerequisites include:

- Active Microsoft 365 tenant and/or Azure subscription with AI capabilities deployed
- Read-only access to Microsoft 365, Entra ID, Power Platform Admin Centre, Defender for Cloud Apps, Azure AI Foundry and Cost Management
- Designated stakeholder responsible for service coordination and governance reviews
- Access to existing AI governance policies or guidelines where available

For further information about our solutions please contact your Insight Account Manager

Sources & References

All statistics and market figures cited in this solution sheet are drawn from verifiable third-party research published in 2025–2026.

[1] IBM – Cost of a Data Breach Report 2025/2026
<https://www.ibm.com/reports/data-breach>
Source for: 20% of organisations traced a breach to shadow AI; £200,000 average added breach cost

[2] European Commission – EU AI Act & Digital Omnibus Timeline (updated June 2026)
<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
Source for: All EU AI Act compliance deadlines; €35M / 7% fine structure; Digital Omnibus amendments (May 2026)

[3] Vision Compliance – Enterprise AI Act Readiness Survey 2026
<https://www.visioncompliance.eu/ai-act-readiness-2026>
Source for: 78% of enterprises are unprepared for EU AI Act obligations

Insight Proprietary & Confidential. Do Not Copy or Distribute. © 2026 Insight. All Rights Reserved