Cyberfort
Expert-led. Security Driven.

AI Security Readiness Review

Fast-track assurance for organisations deploying AI tools

Introduction

Artificial intelligence is being adopted at a pace that security and governance programmes simply have not kept up with. Microsoft Copilot is being rolled out across enterprises in days. ChatGPT accounts are being created by individual employees without IT sign-off. Shadow AI – the use of unapproved AI tools for business tasks is already widespread in most organisations, and many organisations have no clear picture of it.

The problem is not that AI tools are inherently dangerous. The issue is that they are being deployed into environments where data permissions are poorly governed, where staff have access to far more information than their roles require, and where no one has assessed what happens when an AI assistant can surface, summarise, and share that information on request.

Cyberfort's AI Security Readiness Review gives you a clear, expert-led picture of your current AI risk exposure including what tools are in use, what data they can reach, where governance is absent, and exactly what to do about it. In a world where a single misconfigured AI tool deployment can expose sensitive HR, financial, or customer data to anyone who knows how to ask, not knowing is not a safe position.

Key Challenges With AI Security and Governance

Overpermissioned data environments make AI dangerous by default. Most organisations deployed Microsoft 365 without enforcing strict data access controls, because users managing their own files did not create visible risk. When an AI assistant can query the entire SharePoint estate, those latent permissions become an active exposure.

Shadow AI is already in your organisation. Research consistently shows that a significant proportion of employees are using AI tools that have not been approved, assessed, or even identified by IT or security teams. These tools are often free, consumer-grade, and have no enterprise data protection agreements in place.

Governance frameworks have not caught up. Acceptable use policies, data classification schemes, and third-party risk processes were written before generative AI existed. Most do not address LLM usage, prompt data risks, or AI output validation requirements.

Regulatory expectations are hardening. The EU AI Act, the UK Government's AI governance guidance, ICO expectations on automated processing, and sector-specific regulators are all moving in the same direction, they expect organisations to demonstrate they have assessed and governed their AI deployments. That expectation is becoming a compliance obligation.

There is no standard for what "good" looks like. Unlike endpoint security or patch management, AI security is a new discipline with no widely adopted baseline. Organisations do not know what they should be doing and without specialist expertise, they cannot find out quickly.

AI Security in Focus

60%

of organisations have no formal AI acceptable use policy in place

Gartner AI Governance Survey, 2025

3 in 4

Microsoft Copilot deployments reviewed by security specialists contain at least one significant data access misconfiguration at the point of go-live.

Industry Analysis, 2025

These statistics show the speed of AI adoption has outpaced the security and governance frameworks designed to protect organisations from its risks. Waiting for a framework to mature, or for a regulator to act, is not a strategy, it is a liability.

Situations where your business needs this service

This service is especially timely when one or more of the following is true for your organisation:

- You are in the process of deploying or have recently deployed Microsoft Copilot across your Microsoft 365 environment.
- You have recently experienced a fraud attempt involving impersonation or social engineering.
- You are preparing for a cyber insurance renewal, and your insurer has asked about AI governance or data handling controls.
- Your organisation is subject to a regulatory audit, compliance review, or due diligence process, such as ahead of a merger, acquisition, or public sector contract.
- Your board or executive team has been asked to sign off on AI adoption but has no independent assurance that the deployment is secure.
- You have recently experienced a data incident, near-miss, or internal concern related to data access or overpermissioning.
- You are subject to the EU AI Act, FCA, ICO, or other regulatory oversight that is increasingly scrutinising automated processing and AI governance.

Who is this service for?

This service is designed for technology and business leaders who are deploying or planning to deploy AI tools such as **Microsoft Copilot, ChatGPT Enterprise, Claude or other large language model (LLM) platforms**, and who are not yet certain whether the right governance, data controls, and security protections are in place.

It is most relevant to **CIO's, CISO's, CTO's and those who manage company risk profiles**. If you are asking questions like "we've deployed Copilot but do we actually know what data it can access?" or "our staff are using AI tools, do we know which ones, and what they're doing with company data?", this service was built for you.

What does a typical engagement for this service look like?

Cyberfort's AI Security Readiness Review follows a structured, step-by-step approach designed to be low-disruption for your team while producing executive-ready outputs.

1 Step 1 - Scoping and Discovery

Cyberfort works with your IT and security leads to establish which AI tools are in active use across the organisation, both sanctioned and unsanctioned. We agree the scope of the review, identify the key systems and data environments to assess, and establish the baseline questions your organisation needs answered.

2 Step 2 - AI Usage and Exposure Review

Our consultants conduct a structured assessment of how AI tools are being used, what data they can access, and where the highest-risk interactions are occurring. This includes a review of Microsoft 365 and Copilot permission structures, an assessment of shadow AI usage, and an evaluation of any third-party AI integrations in use.

3 Step 3 - Security and Governance Assessment

We assess the controls, policies, and governance processes currently in place against the specific risks created by your AI deployment. We identify gaps in data classification, access controls, acceptable use policy, third-party risk management, and staff awareness, and we rate them by risk severity.

4 Step 4 - Findings, Scorecard, and Roadmap

Cyberfort produces an Executive Risk Scorecard that gives your board and leadership team a clear, jargon-free view of your AI security posture, alongside a practical Remediation Plan that tells your team exactly what to fix, in what order, and why. Governance templates are provided to accelerate remediation.

Key Deliverables of the Cyberfort AI Security Readiness Review

- AI Security Risk Assessment
- AI Usage and Exposure Review
- Governance Templates
- Executive Risk Scorecard
- Prioritised Remediation Plan

Business Value of this service

- Identify AI and LLM security risks before they materialise into incidents or breaches
- Understand what data your AI tools can access and close the gaps
- Establish governance and policy controls that satisfy regulatory and insurance requirements
- Provide board-level assurance over AI adoption with independent, expert-led assessment
- Accelerate safe AI deployment without slowing down the business

Key Outcomes from this service

Organisations that complete Cyberfort's AI Security Readiness Review leave with:

A clear picture of their AI exposure - A structured AI Usage and Exposure Review that maps which tools are in use, by whom, and what data they can access, so you know what you are actually dealing with.

A risk-rated security assessment - An AI Security Risk Assessment that identifies your most significant vulnerabilities and governance gaps, ranked by severity and framed in terms of business impact.

Board-ready assurance - An Executive Risk Scorecard that gives your leadership team a clear, evidence-based view of your AI security posture and what is being done to improve it.

Practical governance tools - Governance Templates covering acceptable use policy, AI risk assessment process, data classification guidance, and third-party AI tool assessment criteria - ready to implement, not to re-draft from scratch.

A clear path forward - A prioritised Remediation Plan that tells your team what to address immediately, what to schedule, and what to monitor, with ownership and accountability built in.

The result is an organisation that has moved from unstructured AI adoption to governed, auditable AI deployment, with the board visibility, documented due diligence, and practical controls that regulators, insurers, and enterprise customers increasingly require.

What our customers say about this service

"Our board wanted assurance that our AI adoption was being managed responsibly. We couldn't answer their questions with any confidence. Cyberfort gave us the Executive Risk Scorecard and the governance framework we needed to go back to the board with a credible, evidenced position."

CTO,
Professional Services Business

"We had staff using all kinds of AI tools that IT had no visibility of. The exposure review was a real wake-up call, not because staff were behaving badly, but because no one had ever told them what was and wasn't appropriate. The governance templates gave us a foundation to build on quickly."

Group Risk Director, following pre-acquisition due diligence review

Next Steps

Your organisation is almost certainly already using AI tools. The question is whether you have the visibility, governance, and controls in place to do so safely. Book a 30-minute call with one of our AI security specialists to understand your current exposure.

Contact us at info@cyberfortgroup.com or call +44 (0)1304 814800 to arrange your call.

To find out more about our full range of cyber security services, visit cyberfortgroup.com