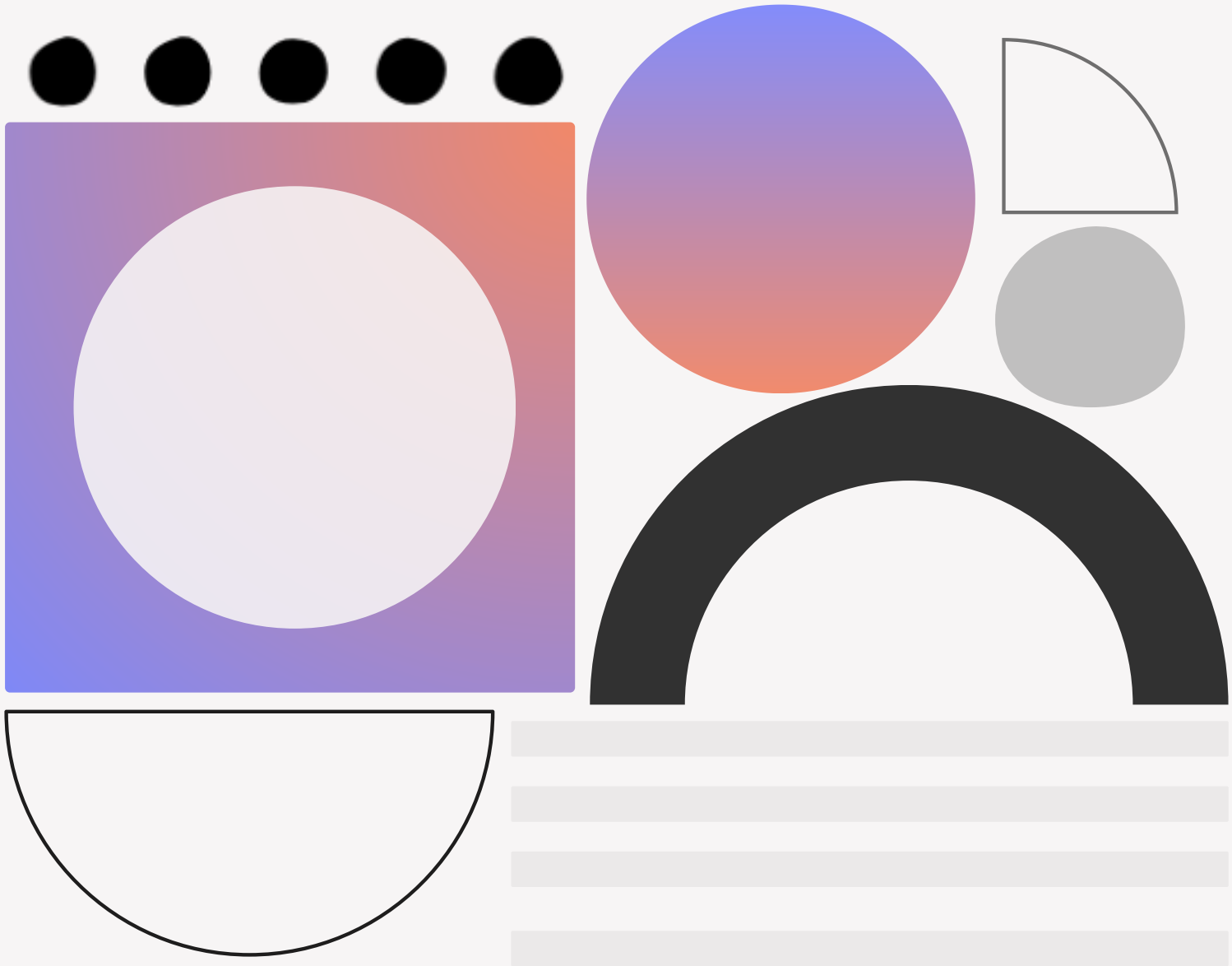
The Data Governance Gap

Exploring the gap between assumed and actual control in Microsoft 365 ahead of AI adoption



For CIOs, COOs, and leaders accountable for risk

Don’t assume control—evidence it

Every organisation carries some degree of data exposure risk. The difference lies in whether they have the visibility and governance to control it properly.

It is easy for data governance to slip as teams grow and platforms evolve But responsible AI adoption requires robust data foundations. Before AI is introduced, instead of assuming policies and controls exist, leaders should evidence them—ensuring they are appropriate, up to date, and consistently enforced across their core environment.

Microsoft 365 environments tend to become more complex as users, processes, and system integrations change. That complexity can increase data exposure risk if permissions, access, and ownership aren’t properly managed and regularly reviewed.

Copilot needs clarity

AI tools like Copilot work with any information they can access—even information that is not meant for public consumption.

Introducing Copilot into a Microsoft environment where data governance is unclear or adhoc, can quickly lead to data exposure and non-compliance.

Copilot works within the security parameters that exist across Teams, SharePoint, OneDrive, and Exchange.

If Copilot is introduced into a Microsoft 365 environment that is built on:

- outdated permissions
- misaligned access
- inconsistent policies

a single prompt can turn private and confidential information into public knowledge.

Before introducing Copilot, leadership teams should be able to confidently evidence data governance processes across Microsoft 365 and the wider organisation, to mitigate AI-related cyber risks and support responsible AI adoption.

Risk exists (before AI even enters the conversation)

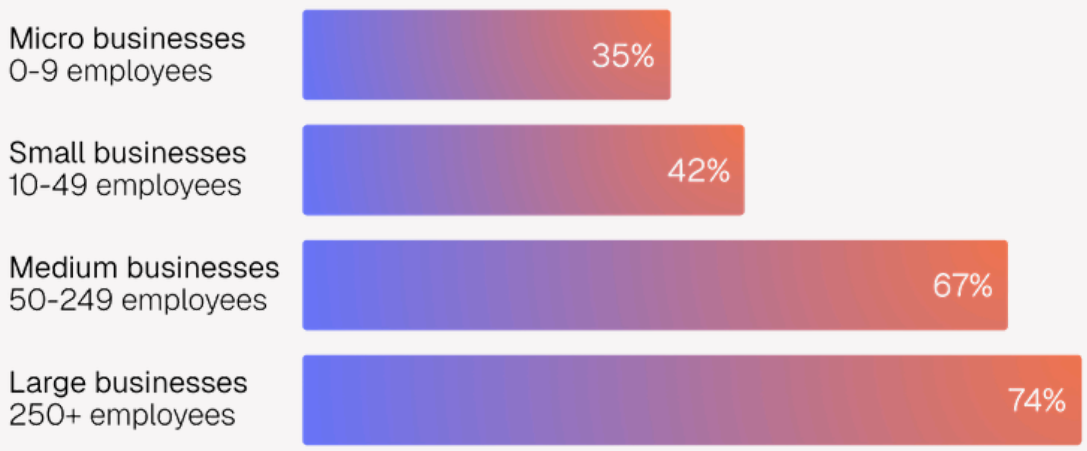
The most recent government Cyber Security Breaches Survey highlighted the prevalence of cyber risk in organisations of all sizes in businesses in the UK.

More than

four in ten

UK businesses reported a cyber breach in 2025[1]

Breaches reported in the past 12 months[1], by organisation size (%)



The report stated that more than four in ten (43%) businesses reported a cyber attack or breach in 2025. For mid-sized firms, that number increased to 67%, while nearly three quarters (74%) of large enterprises reported an incident. These numbers demonstrate how widespread cyber risk is, before AI even enters the conversation.

The way we work is different now

To be clear, this is not suggesting that every data breach results from weak security policies in Microsoft 365. Cyber incidents take many forms and can originate across the wider estate.

The point is that exposure risk is already prevalent. And as cloud environments are central to core operations, communication and productivity, safeguarding them is a business critical task.

In the modern threat landscape, evidencing effective data governance is not something leaders should do only if they are planning to adopt AI.

Embedding robust security measures into environments should be a core requirement in every business, regardless of AI—ensuring controls proportionate, consistent, and actively maintained to protect people, platforms, and data.

[1] **Cyber Security Breaches Survey 2025.** Percentage of UK organisations (by size) that reported an attack or breach in the 12 months prior to the survey publish date.

Day-to-day operations depend on digital workspaces

Microsoft 365 has become a core platform for collaboration and productivity on a global scale.

The millions of active users worldwide demonstrate how embedded Microsoft 365 services are in day-to-day operations, enabling multi-site businesses and hybrid workforces.

Sensitive data is stored, accessed, and shared across cloud platforms and digital workspaces have become the default home for productivity and collaboration.

There are more than

320 million

active users on Microsoft Teams globally[2]

Change is constant

Requirements and workspaces are always changing—often under pressure and tight deadlines.

Practical decisions are made in lieu of best practice to accommodate urgent requests and stakeholder demands.

Everyday actions and ad hoc changes can create a data governance gap over time

Broadening permissions to speed up processes	→ Inherited group permissions granting wider access than required
Granting temporary access (that accidentally becomes permanent)	→ Guest accounts retained beyond their original purpose
Creating a new channel for every project or plan	→ Collaboration spaces without clearly accountable owners
Provisioning SharePoint sites at pace without appropriate policies	→ Inconsistent data structure and sensitivity labels

This is not a criticism of an organisations technical knowledge or intent. It simply reflects what happens organically in the majority of businesses, and demonstrates how easily security controls can weaken over time.

[2] **Microsoft FY23 investor reporting** referencing 320 million monthly active Microsoft Teams users.

Maturity closes the gap—but smaller steps do make a difference

Governance maturity what turns policy into practice, ensuring that controls are actively managed, enforced, and updated.

And yet, only 3% of organisations globally are considered ‘mature’ in terms of cyber readiness[3]—suggesting that maturity is the exception, rather than the norm.

Although developing a mature governance model is the end goal, even baseline controls make a measurable difference.

Only

3%

of organisations are considered ‘mature’ in the context of cyber[3]

A business is

92%

less likely make a cyber insurance claim with Cyber Essentials[4]

Recent statistics published by the UK government support this point.

Research shows that organisations that adopt the Cyber Essentials framework are 92% less likely to claim on their cyber insurance[4] compared with those that do not.

This demonstrates that even through adopting core security controls, accountability improves, and exposure risk reduces—and the same principle applies in Microsoft 365.

Mature governance in Microsoft 365 looks like:

- Defined ownership across Teams and SharePoint preventing unmanaged sites
- Enforced retention and classification policies and supporting lifecycle processes
- Routine access reviews and automated workflows to remove guest access
- Sensitivity labels configured correctly and applied consistently

Mature governance, consistent controls, and clear ownership builds Copilot readiness and creates a stable foundation for responsible AI adoption.

[3] Cisco Cybersecurity Readiness Index 2024.
[4] NCSC Annual Review 2025. Organisations that implement Cyber Essentials are 92% less likely to claim on their cyber insurance.

Closing the governance gap

Your Microsoft 365 environment has been shaped by years of operational decisions. Exposure risk will exist—business leaders must identify where it lies, assess the likelihood of exposure, and be confident that effective controls are in place to prevent data breaches.

The self assessment below will help you validate data governance and identify obvious gaps in security controls ahead of AI adoption. It focuses on four essential areas of governance across Microsoft 365: Access, Ownership, Data Protection, and External Risk.

At the end of the assessment, you will be given an overall readiness score based on your answers, explaining your level of potential exposure risk aligned to each of the core areas, and the steps you can take to strengthen data governance before adopting AI.

Take the self assessment

Identify exposure risk and validate AI readiness in 3 minutes†

The free self assessment will help you build a clearer picture of AI readiness in your organisation, based on your understanding of the data governance processes and controls that currently exist in your environment.

The assessment takes around 3 minutes to complete, and will help you identify:

- Where exposure risk likely exists in your core environment
- Gaps in your governance created by limited visibility, ownership, or structure
- Whether further risk assessment is advised before AI is introduced

Start the self assessment

It is important that you are confident that the controls in question are appropriate for your type/size of business, have defined ownership, and can be demonstrated in practice. Where there is uncertainty, further evaluation is recommended.

†The self assessment is a free and useful tool for establishing AI readiness on a high-level basis. It is not a substitute for an in depth or technical AI readiness assessment. The accuracy of your result is based on your current knowledge and understanding of the governance that exists in your environment.

Remember—control should be evidenced, not assumed

Introducing Copilot (or any AI tooling) into your core operating environment without clear ownership and risk management approach can lead to data exposure or loss. However, many organisations unknowingly have a governance gap in their Microsoft environment—where assumed and actual control are misaligned.

Before introducing Copilot, leaders should assess and evidence:

- External sharing and guest access, including review and removal
- Which Sharepoint and Teams sites are most widely accessible
- Ownership across collaboration spaces and shared sites
- The consistency and accuracy of sensitivity labels in high-risk areas
- Retention policies are applied and enforced correctly
- Accountability for permissions across different groups and roles

If governance is fragile or controls cannot be proven, an AI readiness assessment is the most sensible next step.

Book an AI readiness assessment with 848 Group

At 848 Group, we enable business leaders to strengthen governance and ensure safer, responsible AI adoption—validating security controls, identifying risk across Microsoft 365, and developing a prioritised remediation plan to supports safer Copilot adoption.

Proper governance—not guesswork

For specialist guidance and services across data and AI, the cloud, cyber security and more—visit 848.group

About 848

848 Group works with leadership teams to strengthen governance, reduce operational risk, and ensure technology adoption leads to business outcomes.

Our Microsoft expertise and advisory approach ensure that AI and cloud investments are supported by structured oversight, measurable control, and clear accountability.

Book an AI readiness assessment with 848

Click here to take the self assessment