The Data Security Engagement

Identify data security risks in your organisational data

Partner-led engagement highlights

- Understand the risks of Dark Organisational Data
- Learn about the risks organisational insiders may impose
- Assess your environment against key data protection standards
- Receive an analysis and report on findings and associated risks
- Learn about tools and services that can help mitigate risks
- Explore recommendations and next steps

80%+ **of leaders cited leakage of sensitive data as their main concern around adopting Generative AI**

In today's digital age, data is the lifeblood of any business, and its security is paramount. As the datasphere is projected to double by 2026, the sheer volume and complexity of data will only increase, making it a prime target for security incidents. With the rapid deployment of generative AI apps, data security risks are escalating, demanding robust protection and governance. Yet, an alarming 30% of decision-makers lack visibility into their sensitive data's location or nature, leaving their digital estate vulnerable. It's time to take control and safeguard your business's future. Don't wait for a costly data breach to realize the importance of data security. Secure your data now, and stay ahead in the game of digital defense.

Intelligently investigate and take action on data security risks

Detecting, investigating, and acting on data security risks in your organisation is critical to ensuring trust, creating a safe workplace and protecting company assets and employee and customer privacy.

The Data Security Engagement gives you the insights you need to understand data security, privacy and compliance risks in your organisation.

As your business-critical data expands and generative AI is being deployed rapidly, having an integrated approach that can help quickly identify, triage, and act on data security risks is more important than ever.

By participating in this engagement, our experts will work with you to:

- Document your objectives and strategy around data security, privacy and compliance.
- Show how to detect, investigate and take action on Data security and privacy risks.
- Demonstrate ways to accelerate your compliance journey with the latest Microsoft technologies.
- Provide actionable next steps based on your needs and objectives.

Data Security Engagement

Pre-engagement meeting → Data Security Check → Microsoft Purview Portfolio Overview → Recommendations and Next Steps

Sources: Microsoft Data Security Index report / First Annual Generative AI Study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400

The Data Security Engagement

Identify data security risks in your organizational data

The Data Security Check uncovers risks that might be harmful to your organisation

The Data Security Check is an integral part of the Data Security Engagement. The Data Security Check leverages Microsoft Purview tools and services in an automated process to:

- Discover data that is stored in the Microsoft 365 Cloud and analyse it for the presence of artifacts that may impose data security risks to the organisation.
- Analyze user behavior for events that impose a risk to the customers organization. These vulnerabilities range from the loss of intellectual property to workplace harassment and more.

The Data Security Check is structured around typical Microsoft 365 services and their associated data repositories that organisations use. At its core, the Data Security Check analyses user behavior and scans data repositories related to email, collaboration, and document storage.
Optional modules can be added to extend the Data Security Check to include on-premises data repositories, Windows 10/11 endpoints and more. All activities share a common framework that will allow you to understand the risks that exist in your organisation and develop a roadmap to mitigate and protect your company's information.

Pre-engagement meeting

Data Security Check

Microsoft Purview Portfolio Overview

Recommendations and Next Steps

Mandatory Module	Mandatory Module	Mandatory Module	Mandatory Module
Exchange Online	SharePoint Online	Teams	Insider Risk Management

Optional Module	Optional Module	Optional Module	Optional Module
Compliance Manager	On-premises data stores	Windows 10/11 Endpoints	Communication Compliance

What to expect

By the end of this engagement, experts in Microsoft compliance will provide you with a:

- A Security Check report that includes findings and insights from the automated discovery process.
- A list of recommendations and actionable next steps that will help mitigate the identified risks.
- Clear look into Microsoft's approach to data security and mitigating and controlling insider risks.
- Optional Compliance Manager Tenant Assessment report with suggestions and top key improvement actions.
- Set of long-term recommendations on your compliance strategy, with key initiatives and tactical next steps.

When it comes to security, you need an experienced partner.

To find out how we can support your new ways of working, contact us today.

hello@cps.co.uk
cps.co.uk