



Microsoft Manage and Investigate Risk Workshop

Intelligently identify insider risks

Overview

For most organisations, external cybersecurity risks have been top of mind for many years. But these organisations are now considering the risks posed by trusted insiders as an equal or even more significant threat. Organisations are beginning to recognise the importance of establishing controls to identify and manage insider risks quickly.

Intelligently investigate and take action on insider risks

Detecting, analysing, and acting on malicious and inadvertent activities in your organisation is critical to ensuring trust, creating a safe workplace and protecting company assets.

Our solution

As your business-critical data expands and your workforce shifts to remote work, having an integrated approach that can help quickly identify, triage, and act on risky insider user activity is more important than ever.

Our partner



Related Services

- Insight Microsoft 365 Security Mini-Audit
- Microsoft Threat Protection Workshop

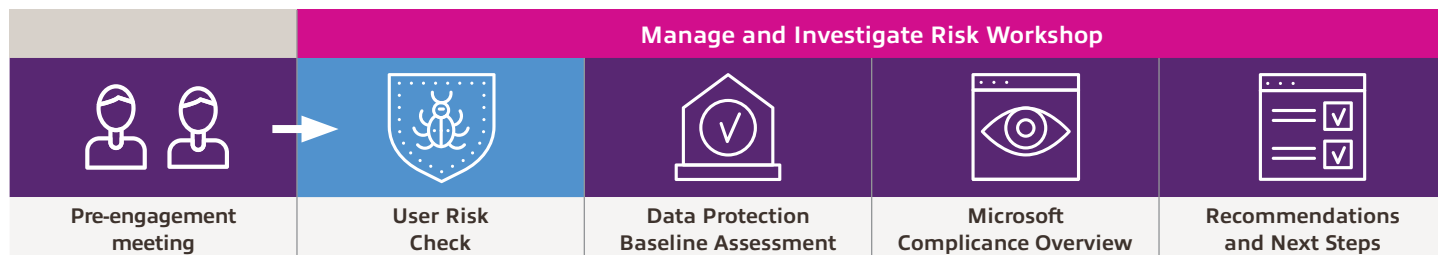
93%

of organisations are concerned about insider risks

The **Manage and Investigate Risk Workshop** gives you the insights you need to understand insider risk in your organisation.

Our experts will work with you to:

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

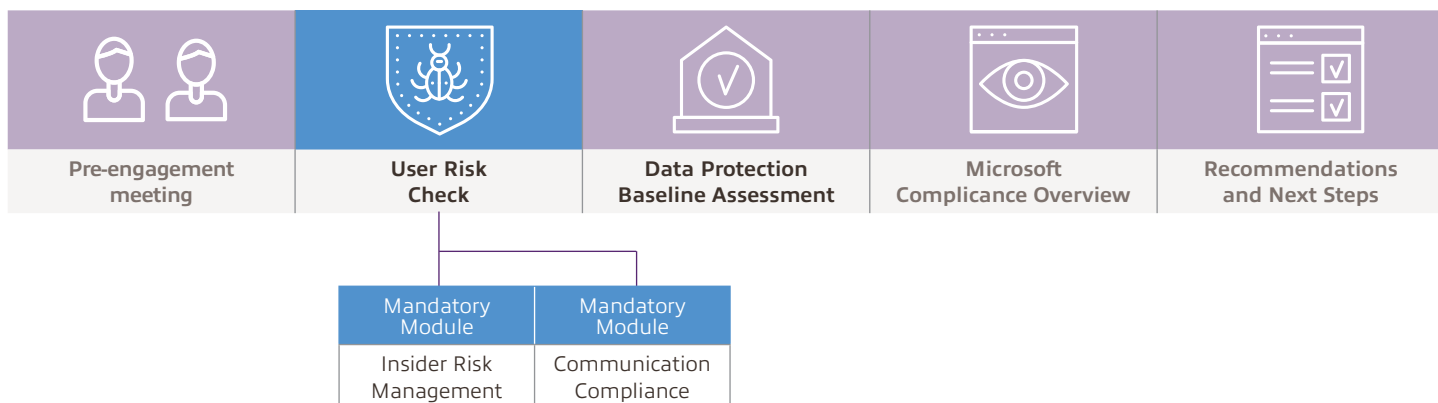


What to expect

The User Risk Check is the core activity of the Manage and Investigate Risk Workshop. The activity is spread out over several weeks to allow time to run on top of your cloud infrastructure and discover and identify insider risks in your organisation. User Risk Check leverages automated Microsoft 365 tools and services to monitor user behaviour and communication to find negligent or malicious behaviour that can impose risk to your organisation.

The automated discovery process will monitor user behaviour and communication for:

- Data leaks, accidental oversharing or malicious intent
- Data Theft by departing employees
- Inappropriate communication and offensive language
- Sensitive information
- Conflict of interest



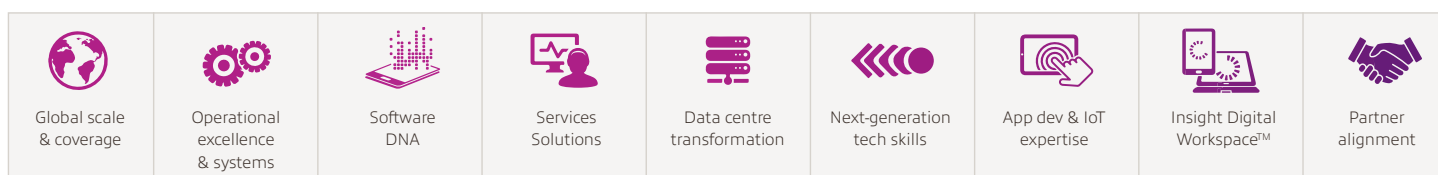
Business outcomes

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

- User Risk 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 mitigating and controlling insider and regulatory risks
- Data Protection Baseline 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

Why Insight?

Today, technology isn’t just supporting the business; it’s becoming the business. At Insight, we help you navigate complex challenges to develop new solutions and processes. We will help you manage today’s priorities and prepare for tomorrow’s needs.



For more information, please contact your Insight Account Manager.

0344 846 3333 | uk.insight.com

