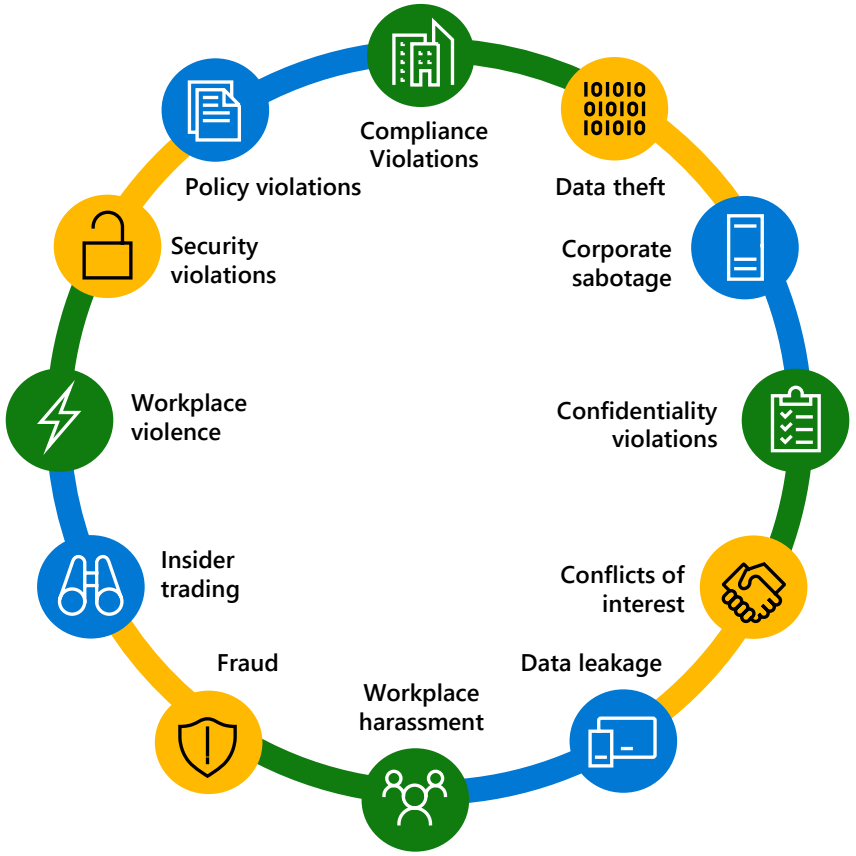
Microsoft Security

Mitigate Compliance and Privacy Risks Workshop

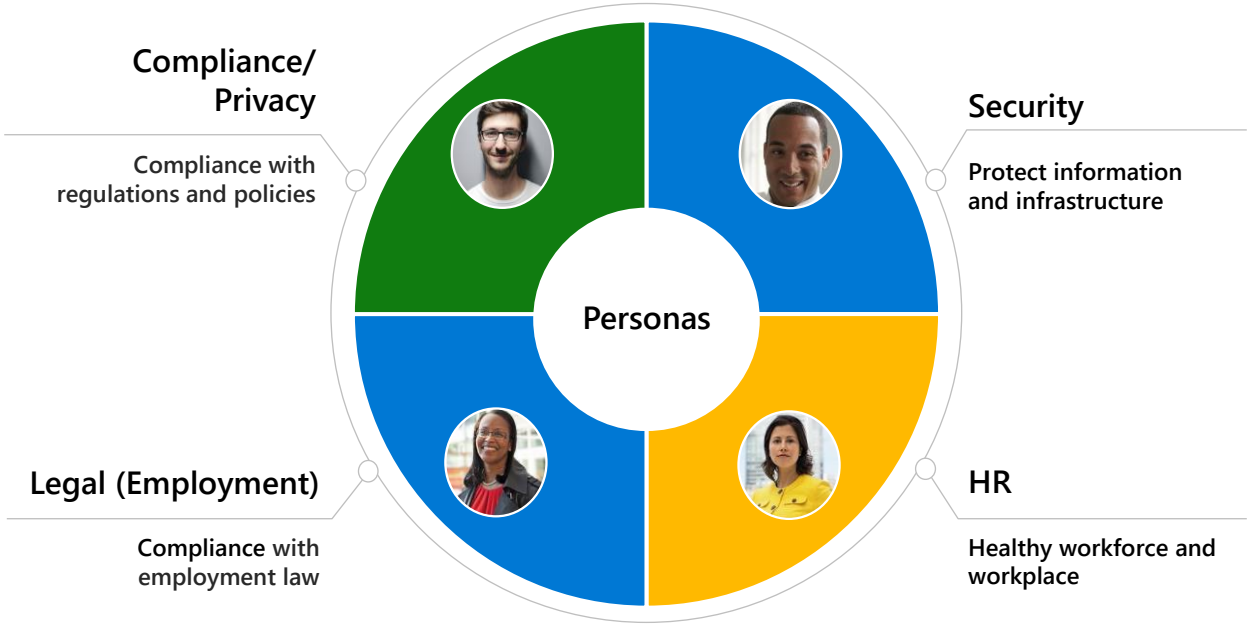
realimpact
TECHNOLOGY CONSULTING

For many years, external threats have been top of mind for organizations, but…

Organizations also face a broad range of risks from insiders…



And many stakeholders are involved in addressing these risks



Insider and communication risks are a universal concern

93%

of organizations are concerned about insider risks[1]

66%

of organizations are "very concerned" about insider risks[1]

$11.45 million

Average cost of insider incidents across industries[2]

77 days

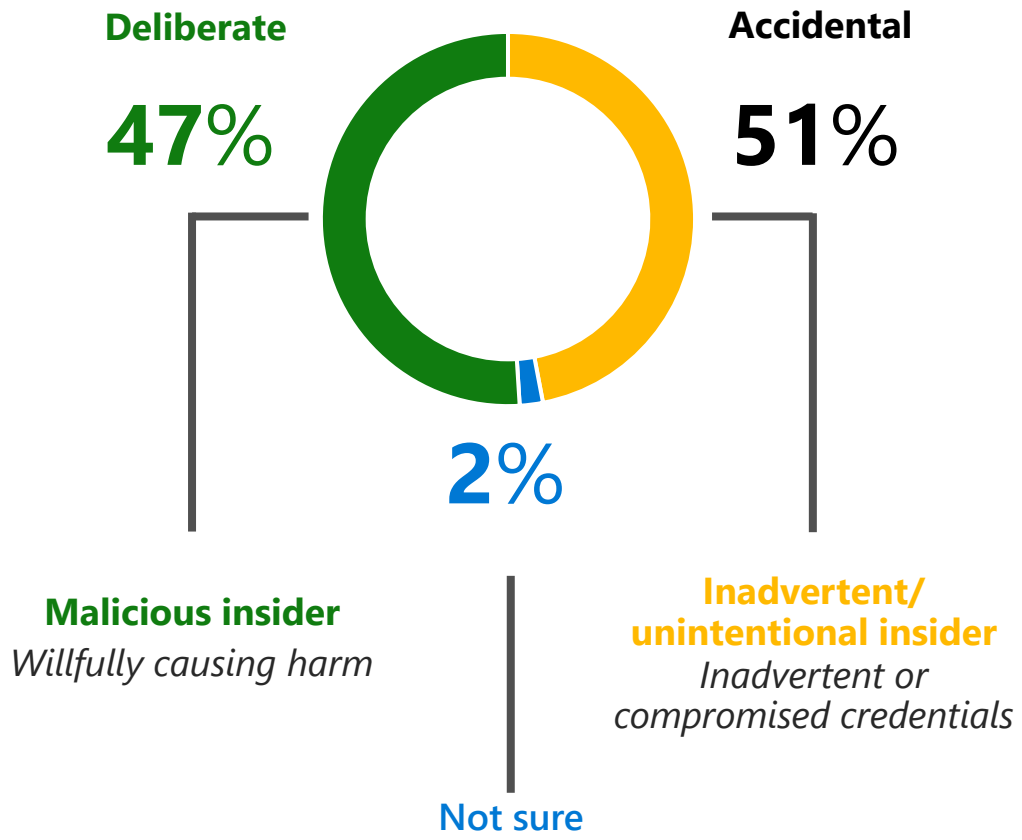
Average duration to contain an insider incident[2]

25%

of data breaches are caused by insiders[3]

[1]Insider Risk Management, Microsoft Market Research, January 2021 [2]2020 Cost of Insider Threats: Global Report, The Poneman Institute. [3]Best Practices: Mitigation Insider Threat, Forrester Report, March 2021

What type of insider are you most concerned about?



Insider Threat Report, 2018

The path leading to a malicious insider risk

Identifying indicators across phases of the critical path can help enable higher fidelity detections.

Predisposition

Tendency to violate policies

51% of employees involved in an insider incident had a history of violating IT security policies leading up to the incident.

Deloitte Metastudy

Stressor

Resignation, demotion, poor review, etc.

92% of insider threat cases were preceded by a negative work event, such as a termination, demotion, or dispute with a supervisor.

Carnegie Mellon CERT

59% of employees who leave an organization voluntarily or involuntarily say they take sensitive data[1]

[1]2016 Deloitte Debriefs "Insider threats: What every government agency should know and do"

Concerning Behavior

Downloads, deletions, anomalous activity, policy violation

97% of insider threat cases studied by Stanford University involved an employee whose behavior had been flagged by a supervisor but the organization failed to follow up.

Deloitte Metastudy

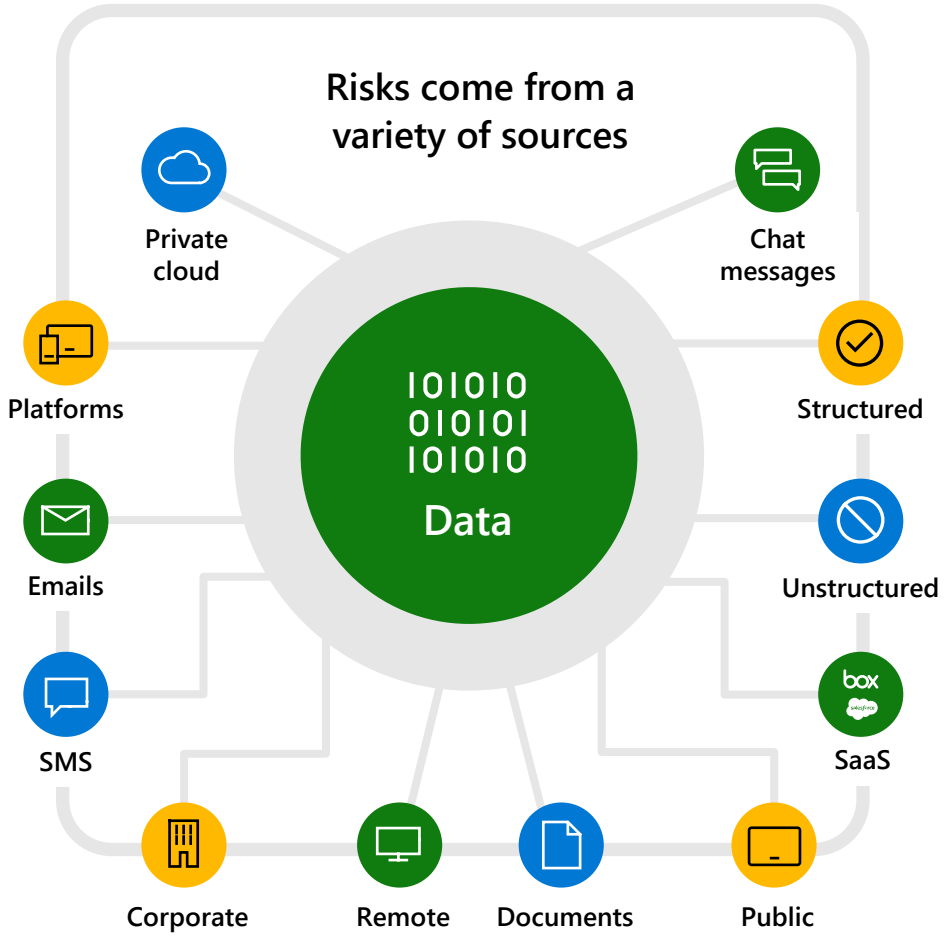
Planning & Preparation

Hiding, renaming, tampering, use of unapproved apps/devices, denied access/errors, after-hours USB activity

59% of employees who leave an organization voluntarily or involuntarily say they take sensitive data with them.

Deloitte Metastudy

Fragmented approach to identifying and managing risks



Risks are difficult to identity and manage

Traditional approaches have limitations

- Configurations requiring scripting
- Deployment of endpoint agents
- Scale and performance issues
- Low visibility into content
- Low sentiment analysis
- Limited signal correlation

UEBA
(User and entity behavior analytics)

UAM
(User activity monitoring)

DLP
(Data loss prevention)

The risks of not being in control of insider risks

Reputational damage

Do you want to be the organization in the news?
What would you like to be known for?
Do people still want to work for you?

Loss of intellectual property or business secrets

What if your company jewels are lost or stolen?
Unintended oversharing or malicious intent, is it happening in your organization?

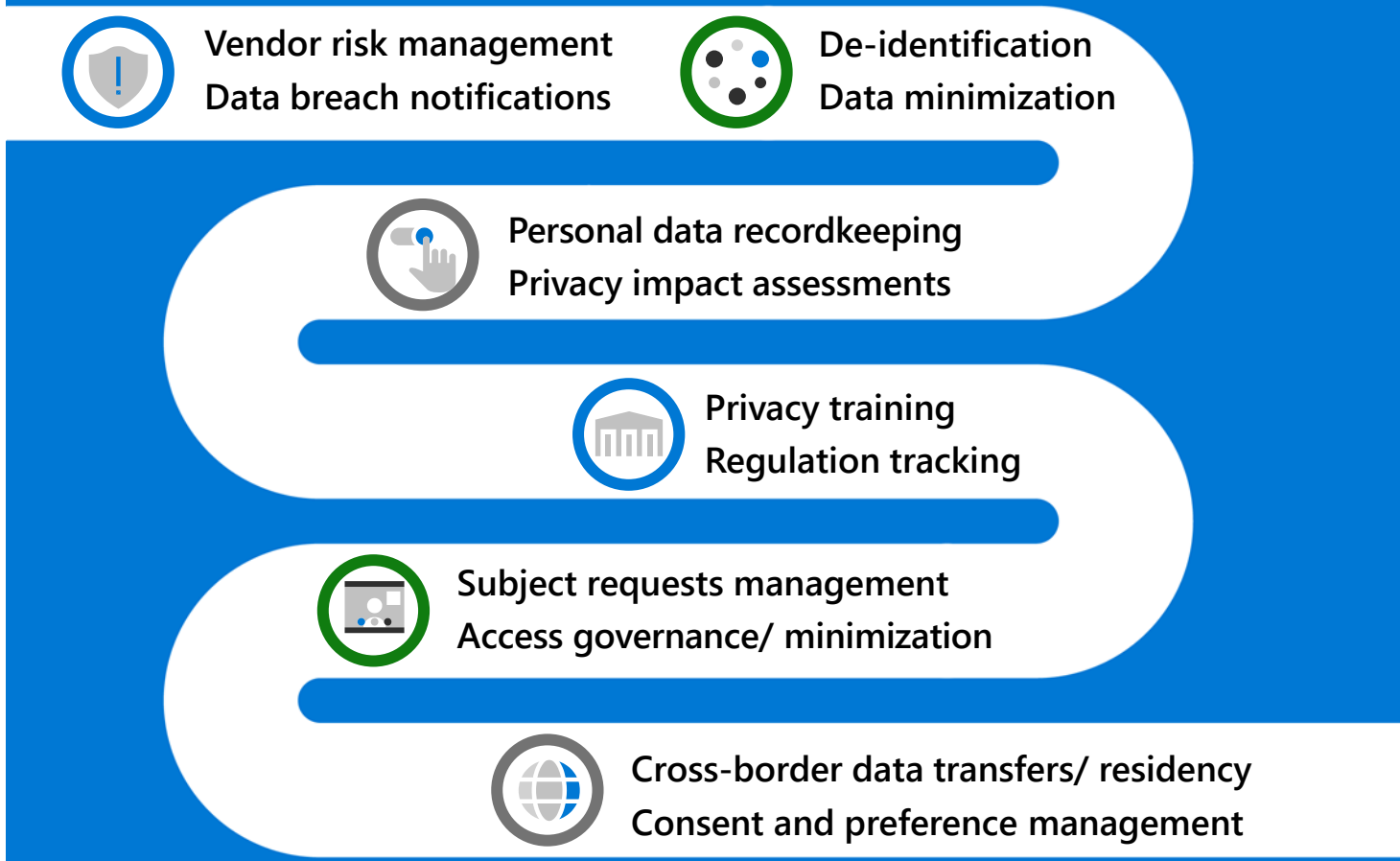
Loss of trust

Is your customers' data safe with you?
Do customers still want to work with you if you lose their trust?

Fines

Can be significant and are real

Organizations need to manage numerous requirements to safeguard customer & employee privacy

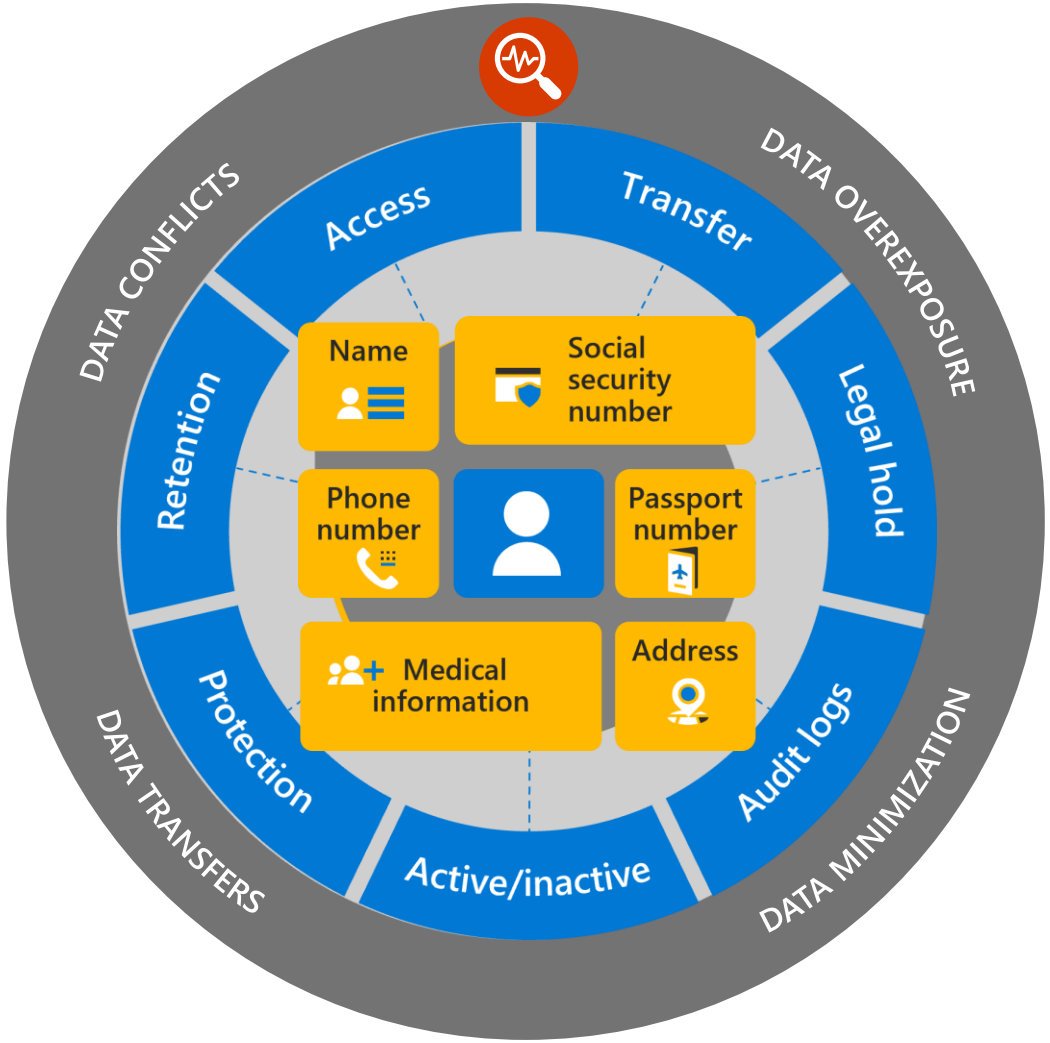


Privacy challenges are everywhere

Can you identify critical privacy risks and conflicts?

Are you able to automate privacy operations and responses to subject rights requests?

Are your employees empowered to make smart data handling decisions?



The need for a privacy-resilient workplace

Information workers need to stay productive and comply with data protection and privacy legislation

Data breaches have increased in number and sophistication over the last few years

58%

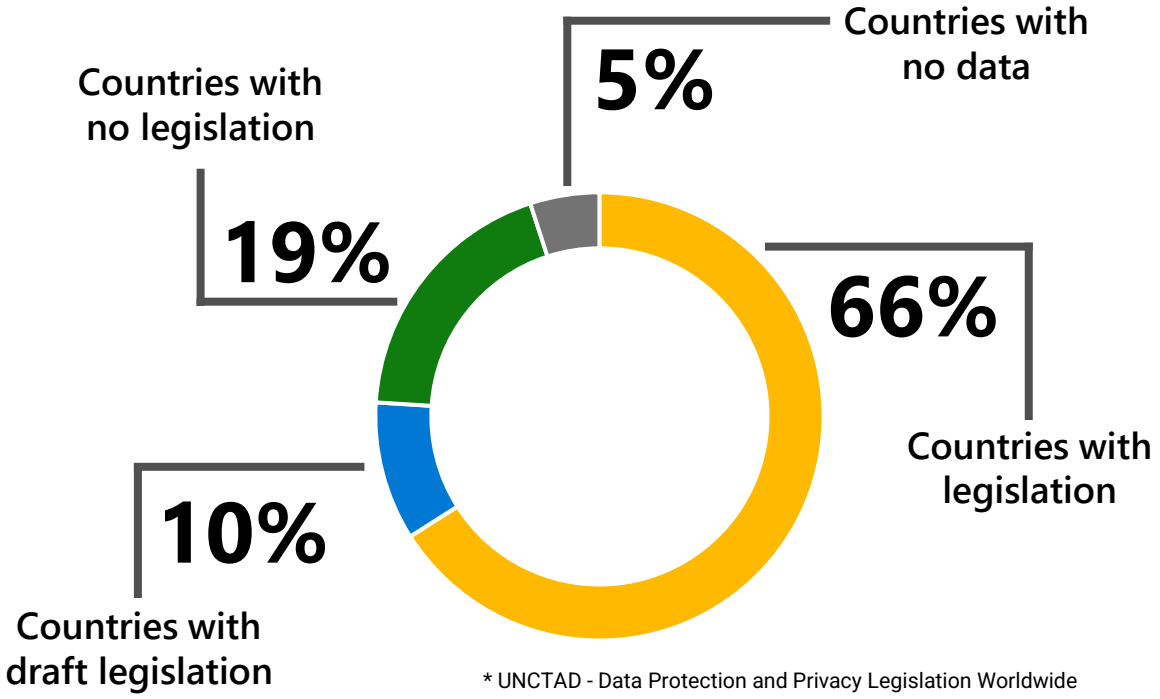
58% of data breaches in 2020 involved personal data

70%

70% of US adults feel their personal information is less secure than 5 years ago

Customers are losing trust in organizations and technology that handle private data

Governments are responding



* UNCTAD - Data Protection and Privacy Legislation Worldwide

What is the User Risk Check?

It’s an automated process that leverages Microsoft 365 products and services to identify risks and vulnerabilities related to organizational insiders and privacy.

The User Risk Check

Enable and configure

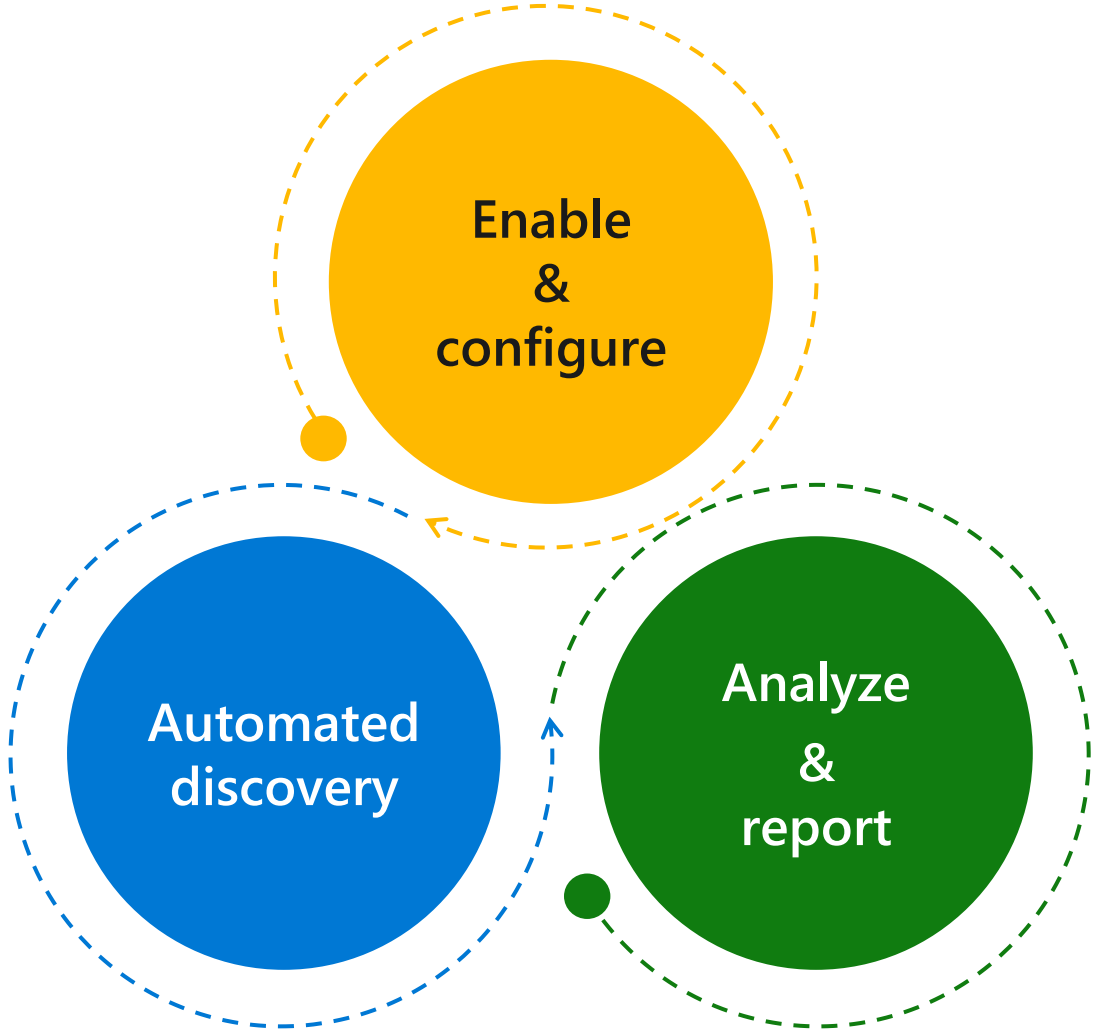
Enable the services for **automated discovery, configure** the **monitoring policies.**

Automated discovery

Two weeks of **monitoring** user communications and user behavior to identify risks and vulnerabilities.

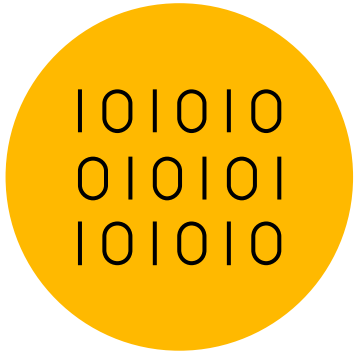
Analyze & report

Analyze the findings and **report** on the insider risks and vulnerabilities that are discovered.



What Automated Discovery looks for

Default scope – mandatory modules



Common data leakage scenarios

General data leaks, data theft by departing users

Communications content

Offensive language, sensitive information, conflict of interest

Out-of-box sensitive info types

Microsoft 365 includes 200+ sensitive info types

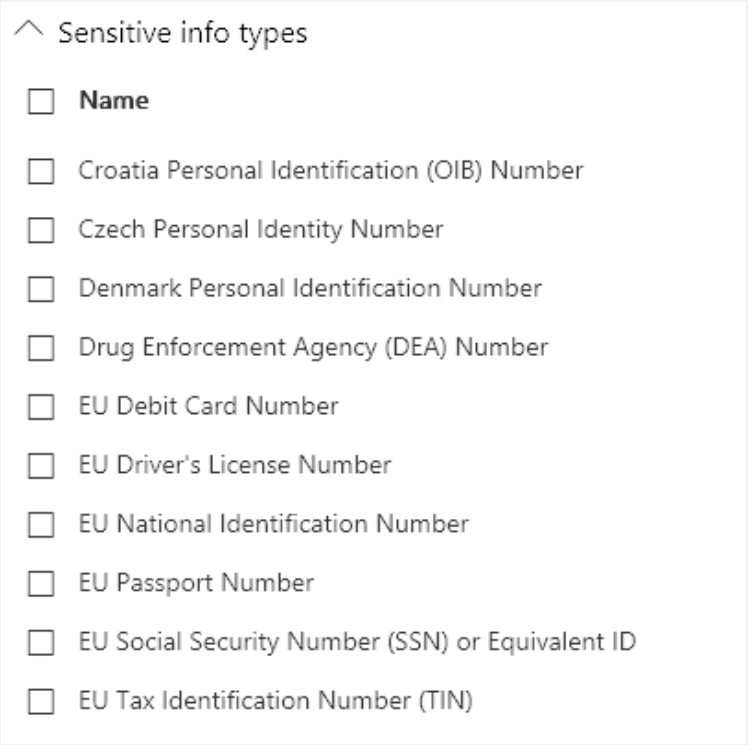
For different countries, industries, or by information type

Sensitive information comes in many forms

Financial data, Personally Identifiable Information (PII)

Examples

- Croatia Personal Identification (OIB) Number
- EU Debit Card Number
- EU Passport Number
- US Driver's License Number
- Social Security Number



Customer-specific sensitive info types

Business intellectual property
Business plans, product designs, confidential projects

Employee or customer information
HR Information, resumés, employment records, salary information

Highly confidential information
Mergers and Acquisition, workforce reduction

Examples

- Employee or customer numbers — *Technology: RegEx*
  - <EMP-nnnnn>
  - <CUST-nnnnnn-NL>
- Specific keywords — *Technology: Static Keywords*
  - <Project Enigma>
  - <Highly Confidential>
  - <Internal only>

Compliance Manager Tenant Assessment

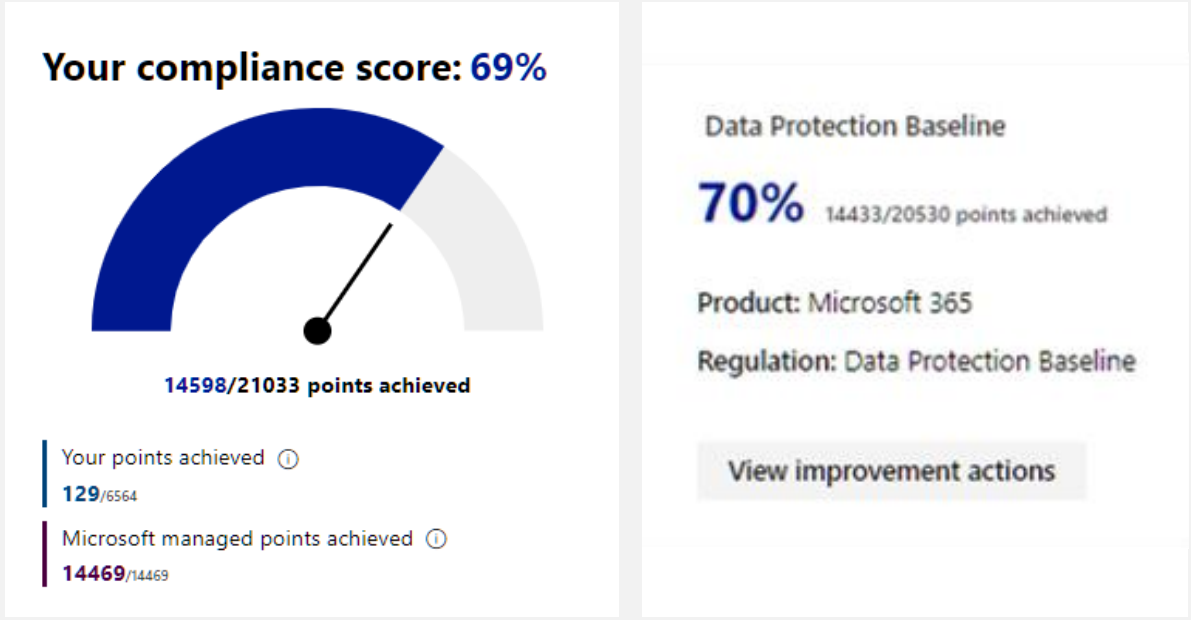
Assess performance relative to key data protection standards and regulations.

Generic and customer specific assessments

- Data Privacy Baseline Assessment
- Premium assessments that align to customer specific requirements
  - Aligned to Region, Industry or type of organization
  - Over 300+ assessments to chose from

Recommendations for improvement together with implementation guidance.

New and updated scenarios are published regularly.



How the Mitigate Compliance and Privacy Risks Workshop can help

Understand the risks organizational insiders may impose
Learn how to identify and respond to insider communications and behaviors that can impose risks on the organization.

Discover insider and privacy risks in your organization
Provide insight into the risks that exist in your organization.

Assess your Microsoft 365 environment
Assess against a set of controls for key regulations and standards for data protection and general data governance.

Analyze and report
Analyze the findings and risks. Provide insight and highlight those that are most impactful.

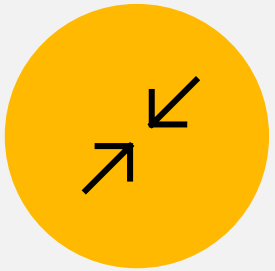
Learn about tools and services that can control and mitigate risks
How cloud services can help and what this means for the end user.

Recommendations and next steps
Provide recommendations for risk mitigation and define actionable next steps

Engagement Objectives

Mitigate Compliance and Privacy Risks Workshop

What we'll do during the workshop



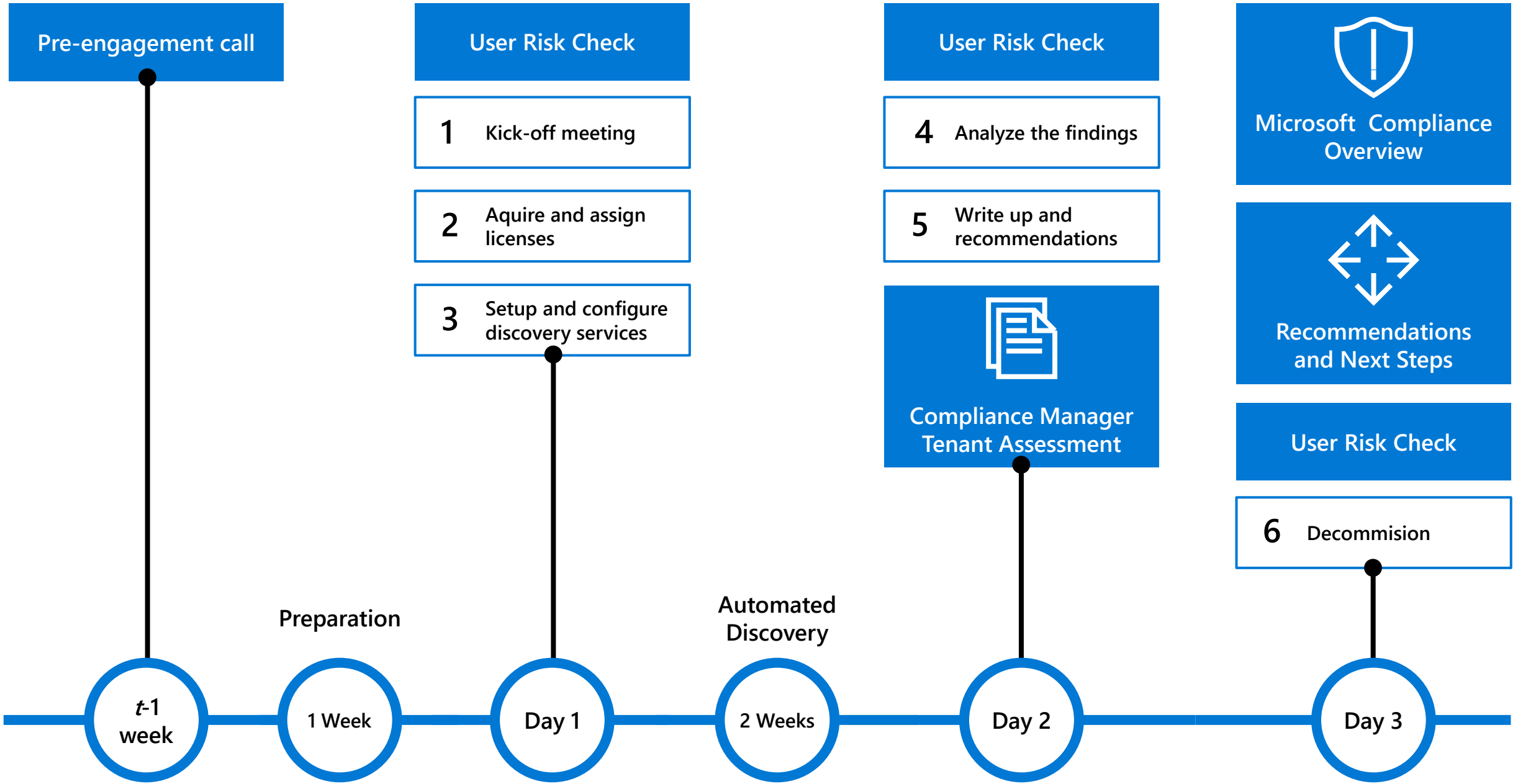
Focus on learning about your priorities, initiatives, and key influences on your compliance strategy

Discover Insider and Privacy Risks in your environment

Learn about Microsoft's approach to compliance and insider risk

Plan next steps on how we can work together

Workshop timeline



Q&A

Microsoft Security

Thank you

real impact
TECHNOLOGY CONSULTING