Gold
Microsoft
Partner
Microsoft

Exelegent

Manage and Investigate Risk 3-Week Workshop

by Exelegent & Microsoft

Exelegent

Exelegent

http://www.exelegent.com/ · in · 36 W Main Street, Suite 300, Freehold, NJ, US 07728

CONTACT >

Search for other providers

This provider has demonstrated competency in the following areas

Gold	Communications
Gold	DevOps
Gold	Data Analytics
Gold	Data Platform
Gold	Cloud Productivity
Gold	Security
Gold	Cloud Platform
Gold	Windows and Devices
Gold	Collaboration and Content
Gold	Messaging
Silver	Small and Midmarket Cloud Solutions
Silver	Enterprise Mobility Management
Silver	Application Development
Silver	Project and Portfolio Management
Silver	Datacenter

10 -Time Gold Microsoft Partner

About us

Exelegent is a cyber security and professional services company where efficiency is standard, and our customers are our partners. Headquartered in Freehold, NJ with supporting offices in Newark, NJ and L'viv Ukraine, Exelegent leverages years of experience to bring about a world-class experience for our clients.

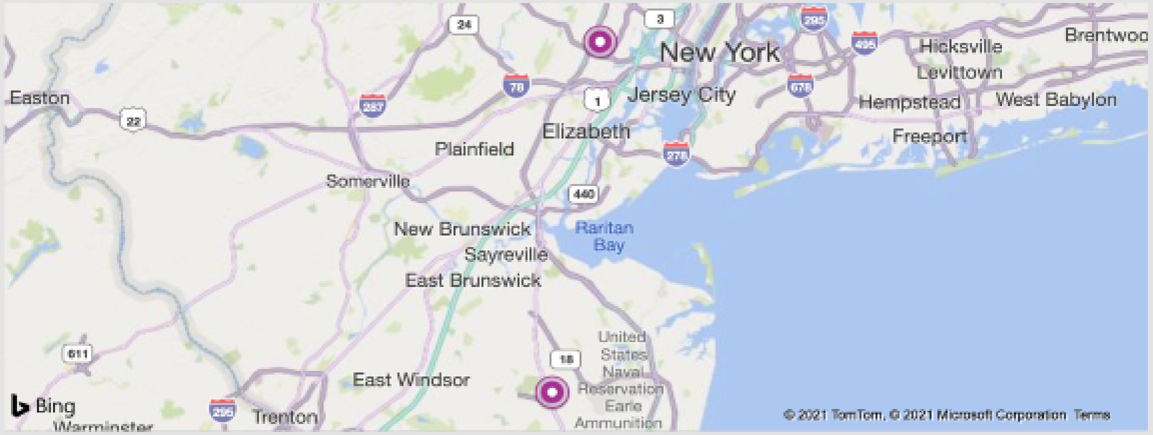
Our specialties include:

More

Skills and Capabilities

- Advanced Analytics
- Agriculture, Forestry, & Fishing
- Application Integration
- Artificial Intelligence
- Azure
- Azure Security & Operation Management

Top locations



36 W Main Street, Suite 300, Freehold, NJ, US 07728

495 N 13th street, Newark, NJ, US 07107

What our clients say:

- "Exelegent helped our company migrate from G-Suite to Microsoft Office 365 with zero downtime and zero data loss. During the process, over 3,500 users continued to collaborate and run critical business functions seamlessly."

  Robert Florescu, CISO, CityMD

- "Switching to Exelegent has been a major contributing factor to the growth of our group. As a company looking to expand, we really value our employees' time and productivity. Exelegent's IT Support has enabled our business to run as efficiently as possible."

  Bruce Lucarelli, CTO, DermOne

- "Exelegent has been with our hospital since we've opened our doors. Their experience in a wide range of projects and solutions, and management of vendors has made a tremendous impact on our efficiency"

  Alexey Gololobov, CFO, Columbus Hospital LTACH

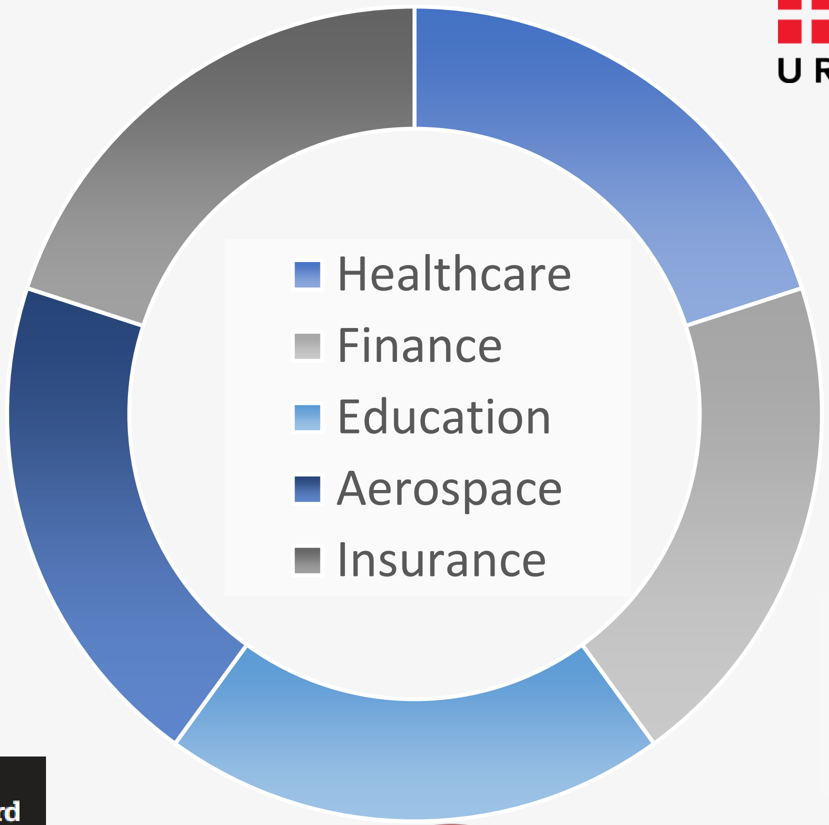
- "Exelegent has become our trusted business partner and completed migration on time, alleviated hosting responsibilities, and gave us capabilities to enable team productivity and data security.«

  Kevin Hannigan, President, ACC Inc.

Exelegent

Clients

Industries we serve



World Insurance

CityMD Urgent Care

Saint Peter's University

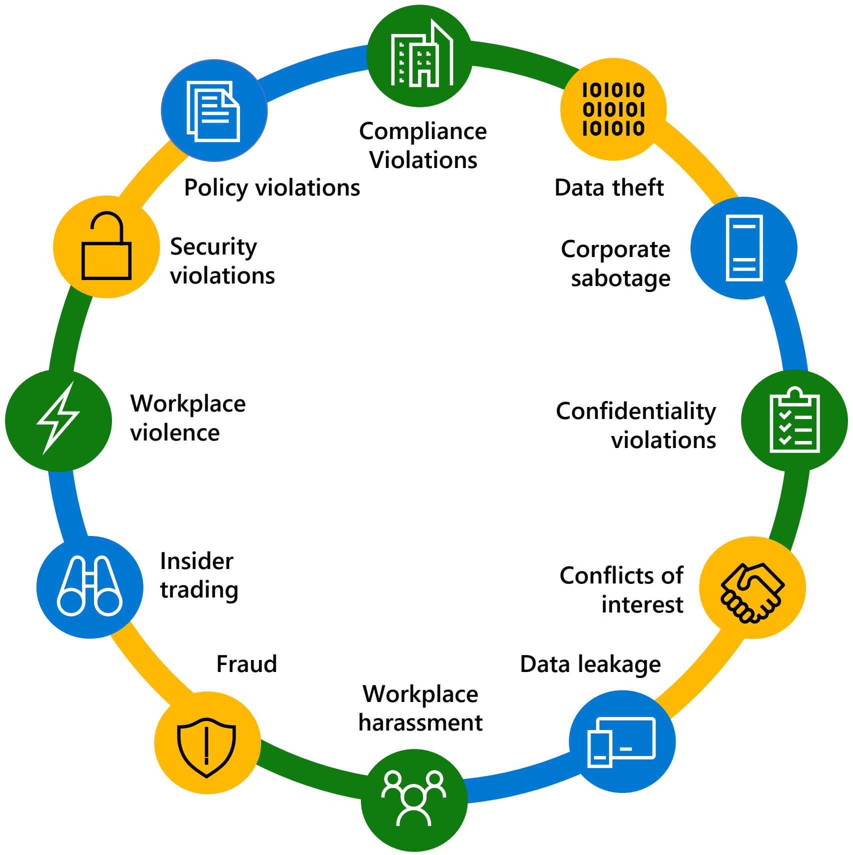
In-Phase Technologies, Inc.

OceanFirst Bank

CollegeBoard

ETS

Organizations face a broad range of risks from insiders…



Compliance Violations

Data theft

Corporate sabotage

Confidentiality violations

Conflicts of interest

Data leakage

Workplace harassment

Fraud

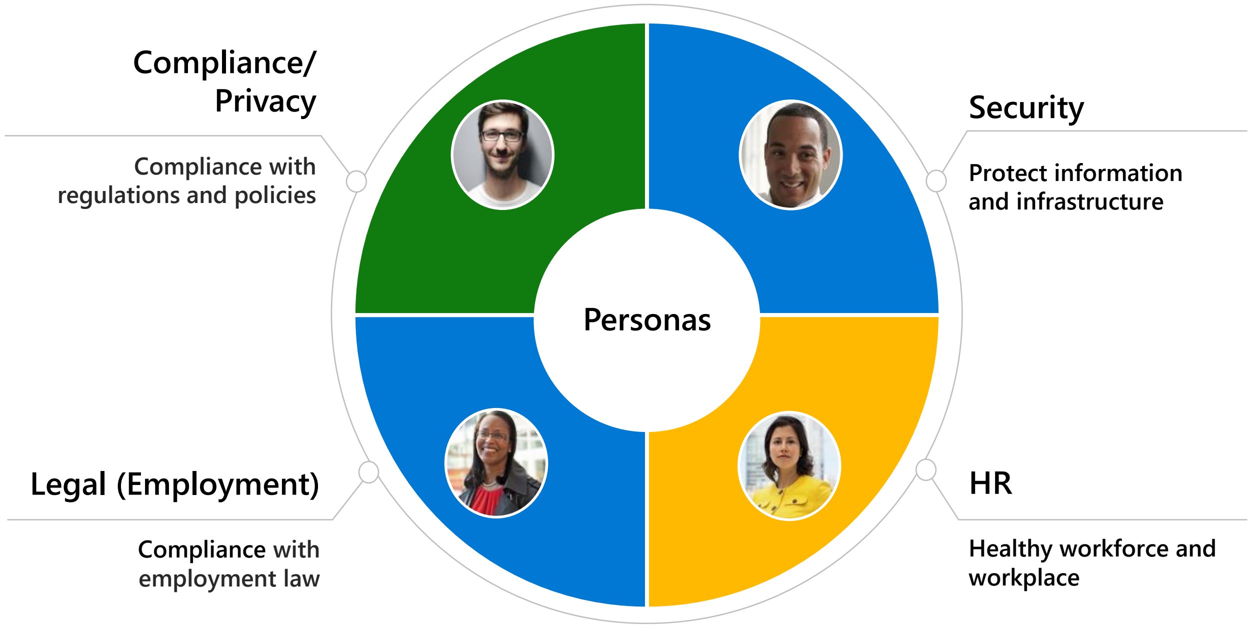
Insider trading

Workplace violence

Security violations

Policy violations

And many stakeholders are involved in addressing these risks



Personas

Compliance/ Privacy

Compliance with regulations and policies

Security

Protect information and infrastructure

Legal (Employment)

Compliance with employment law

HR

Healthy workforce and workplace

Exelegent

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]

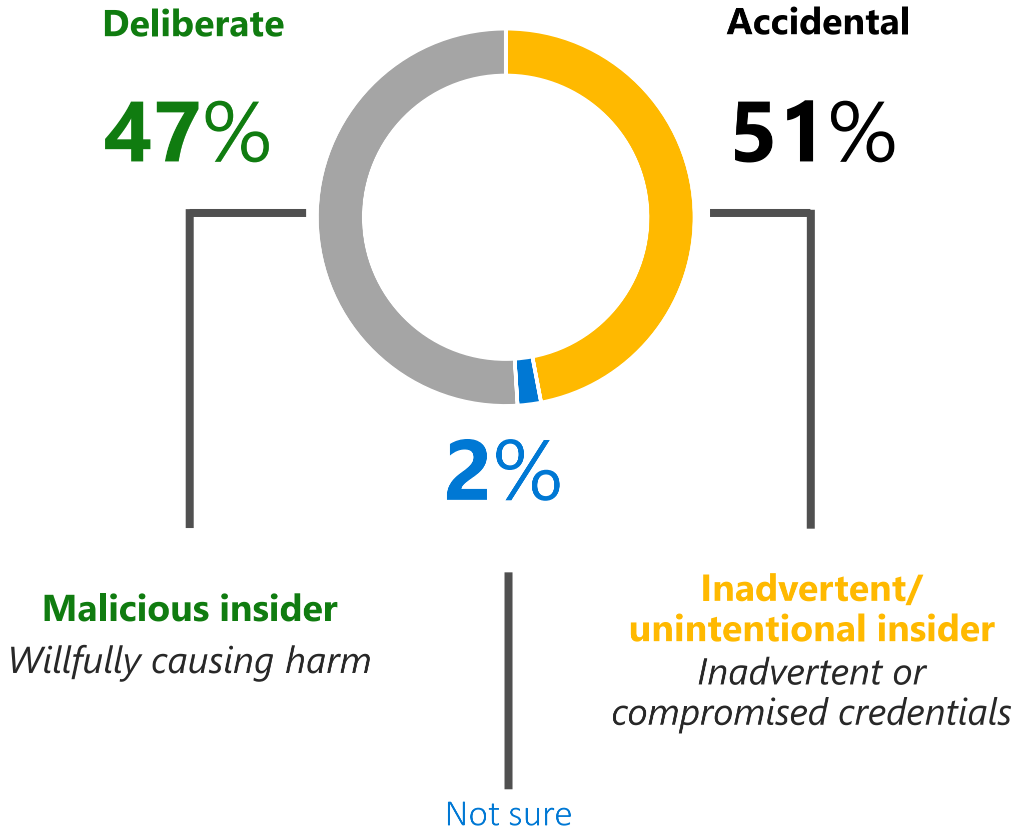
77 days

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?



Deliberate

47%

Malicious insider

Willfully causing harm

Accidental

51%

Inadvertent/ unintentional insider

Inadvertent or compromised credentials

2%

Not sure

Insider Threat Report, 2018

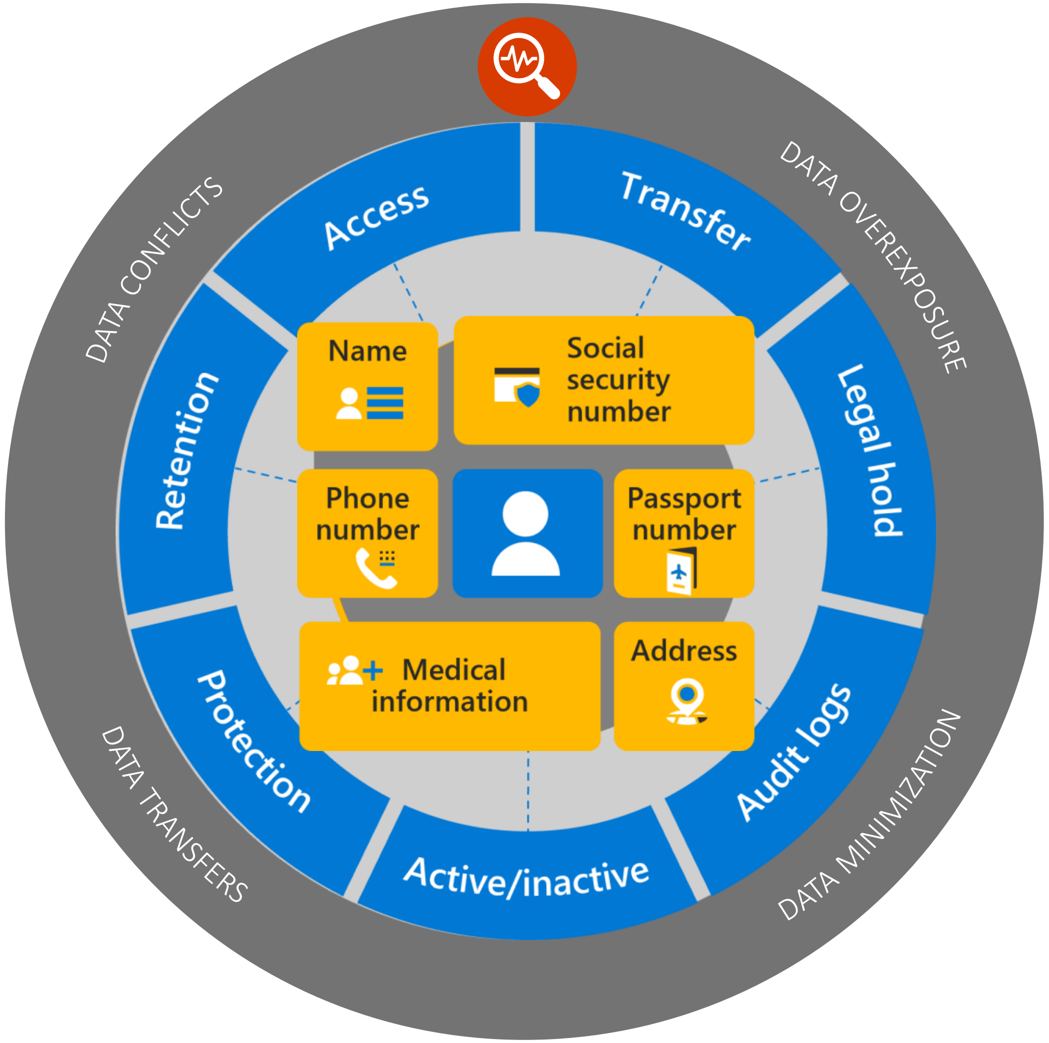
Exelegent

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?



Exelegent

Click to edit Master title style

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.

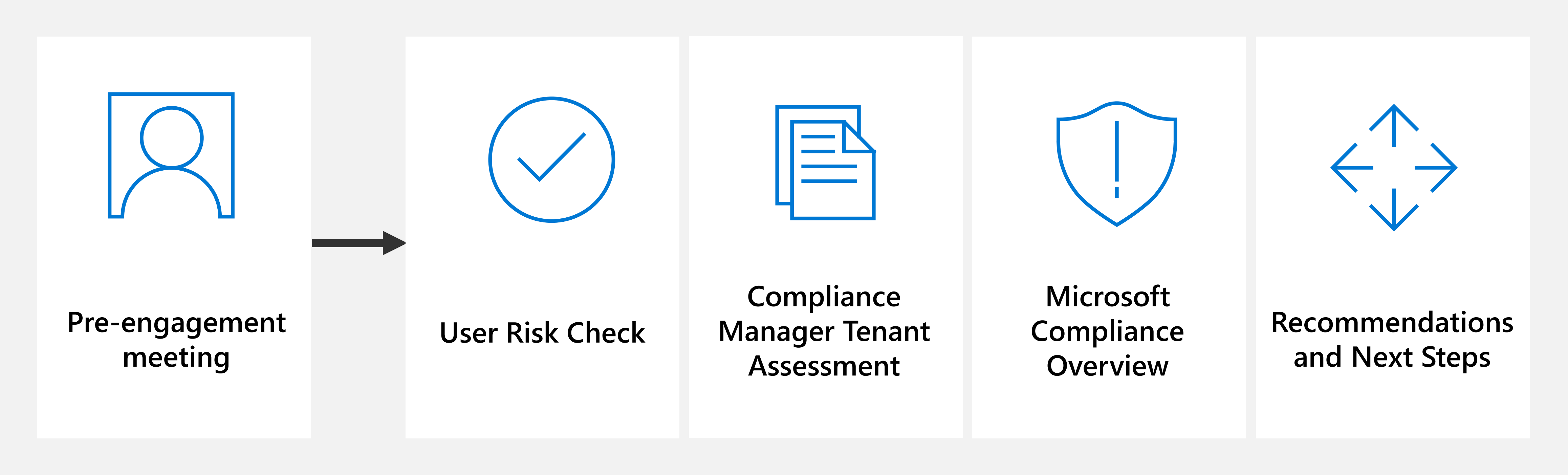
Recommendations and next steps
Provide recommendations for risk mitigation and define actionable next steps

Engagement Objectives

Manage and Investigate Risk Workshop

Exelegent

The Manage and Investigate Risk Workshop



Pre-engagement meeting

User Risk Check

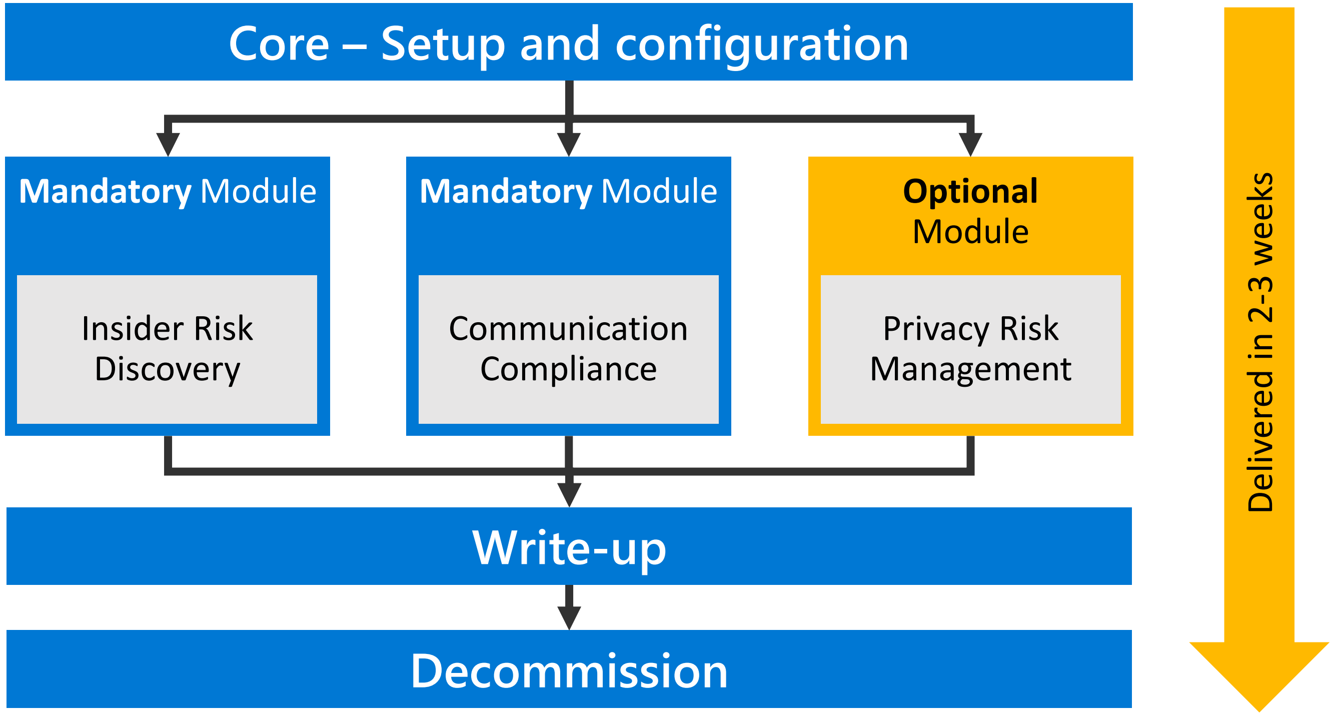
Compliance Manager Tenant Assessment

Microsoft Compliance Overview

Recommendations and Next Steps

Exelegent

User Risk Check’s modular design



Core – Setup and configuration

Mandatory Module

Insider Risk Discovery

Mandatory Module

Communication Compliance

Optional Module

Privacy Risk Management

Write-up

Decommission

Delivered in 2-3 weeks

What’s included

For the User Risk Check activity

Enabling User Risk Check Discovery Services

Insider Risk Management
Communication Compliance
Optional:
Sensitive Information Types, Data Loss Prevention, Privacy Risk Management

Monitoring behavior and communications

Standard: Microsoft 365 audit log, Exchange, SharePoint, Teams, Office, and more
Optional: Devices, Data Loss Prevention, HR Connector

Analysis and reporting

Collect reports, logs, and dashboard information.
Analyze findings, map to solutions, and provide recommendations.

Module - Insider Risk Discovery

Activity overview

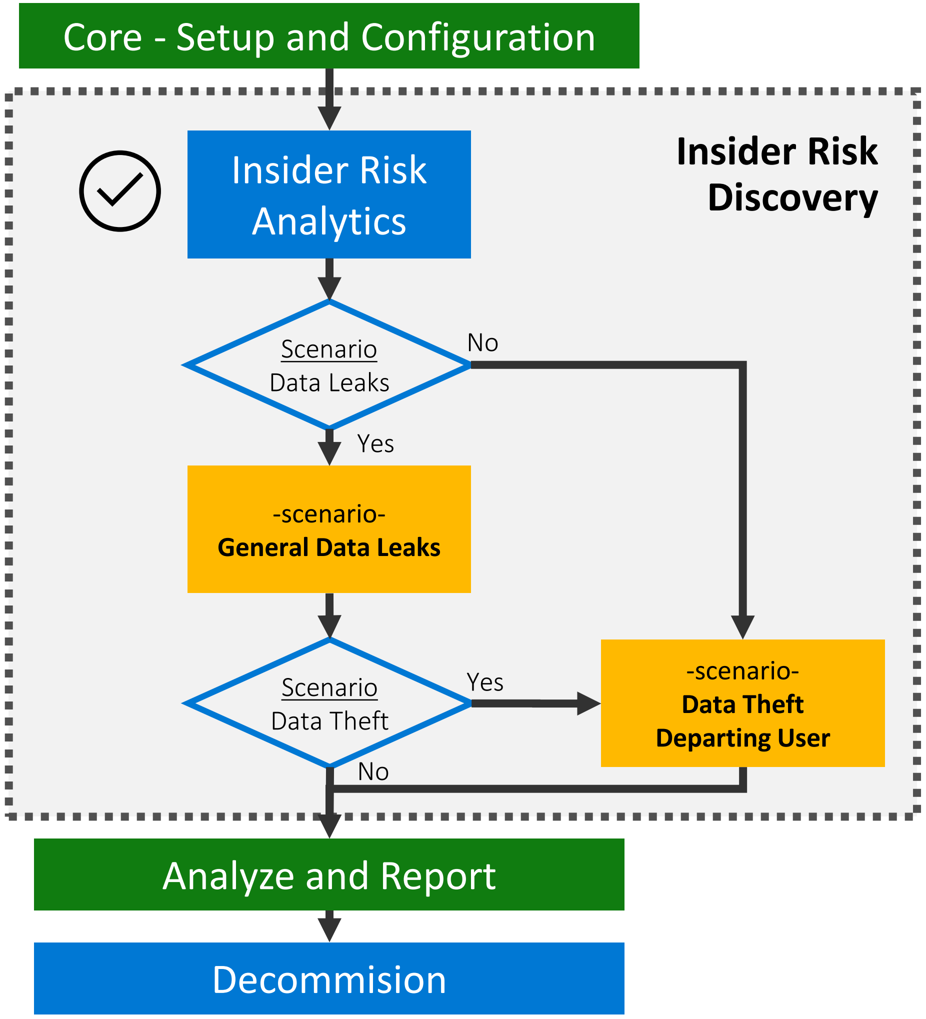
Detect malicious and inadvertent activities in the organization by enabling Insider Risk Management and configuring policies that will define the types of risks to identify and detect.

Insider Risk Analytics

- The first activity for Insider Risk Management

Choose at least one of the additional scenarios:

- General data leaks
- Data theft by departing user



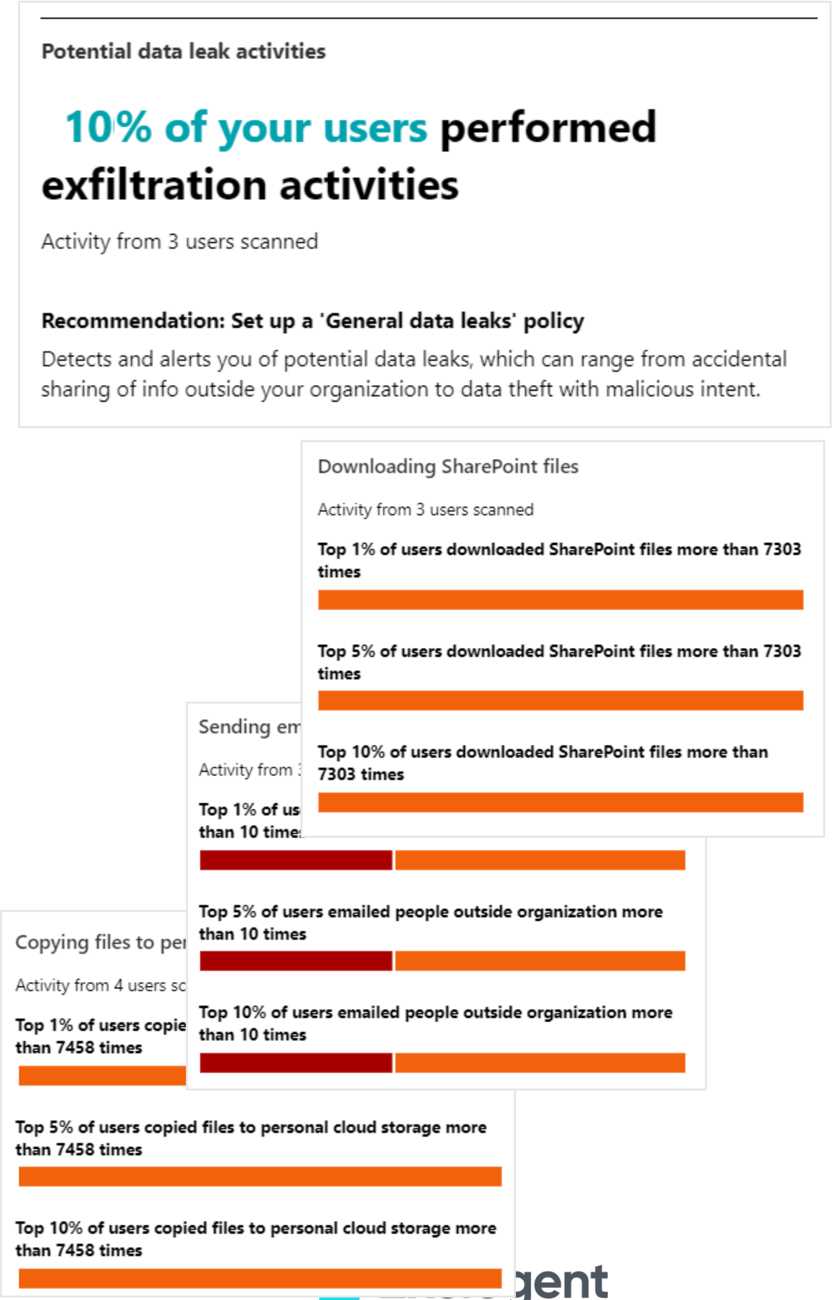
Exelegent

Insider Risk Analytics

Module – Insider Risk Discovery

Evaluation of potential insider risks

- First activity for Insider Risk Discovery
- Insights based on the same signals used by insider risk management
- Works out of the box without configuring policies
- Identify potential areas of high user risk
- Help determine type and scope for policies to consider



Potential data leak activities

10% of your users performed exfiltration activities

Activity from 3 users scanned

Recommendation: Set up a 'General data leaks' policy

Detects and alerts you of potential data leaks, which can range from accidental sharing of info outside your organization to data theft with malicious intent.

Downloading SharePoint files

Activity from 3 users scanned

Top 1% of users downloaded SharePoint files more than 7303 times

Top 5% of users downloaded SharePoint files more than 7303 times

Top 10% of users downloaded SharePoint files more than 7303 times

Sending em

Activity from 3

Top 1% of us than 10 time

Top 5% of users emailed people outside organization more than 10 times

Top 10% of users emailed people outside organization more than 10 times

Copying files to per

Activity from 4 users sc

Top 1% of users copie than 7458 times

Top 5% of users copied files to personal cloud storage more than 7458 times

Top 10% of users copied files to personal cloud storage more than 7458 times

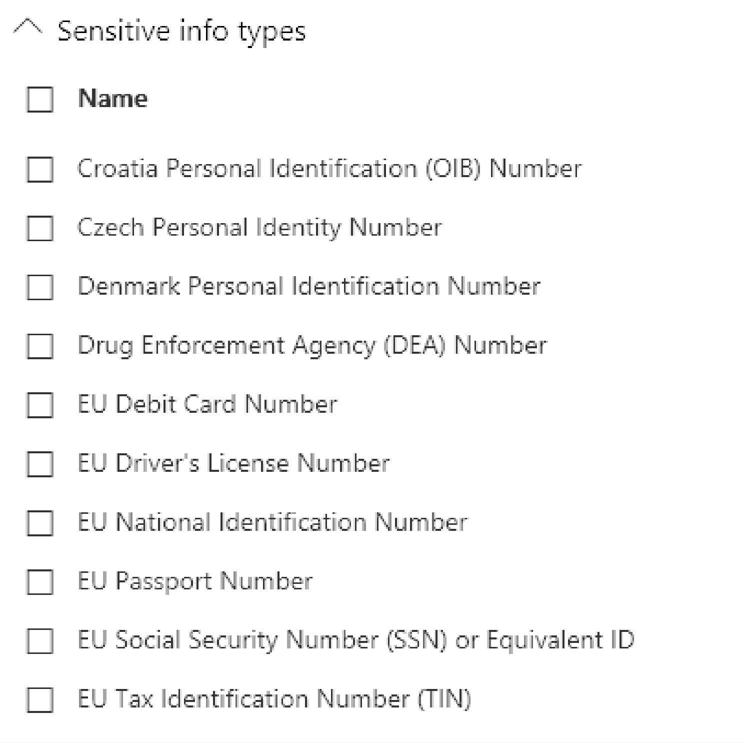
Out-of-box sensitive info types

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



Sensitive info types

□ **Name**

□ Croatia Personal Identification (OIB) Number

□ Czech Personal Identity Number

□ Denmark Personal Identification Number

□ Drug Enforcement Agency (DEA) Number

□ EU Debit Card Number

□ EU Driver's License Number

□ EU National Identification Number

□ EU Passport Number

□ EU Social Security Number (SSN) or Equivalent ID

□ EU Tax Identification Number (TIN)

Module - Communication Compliance

Activity overview

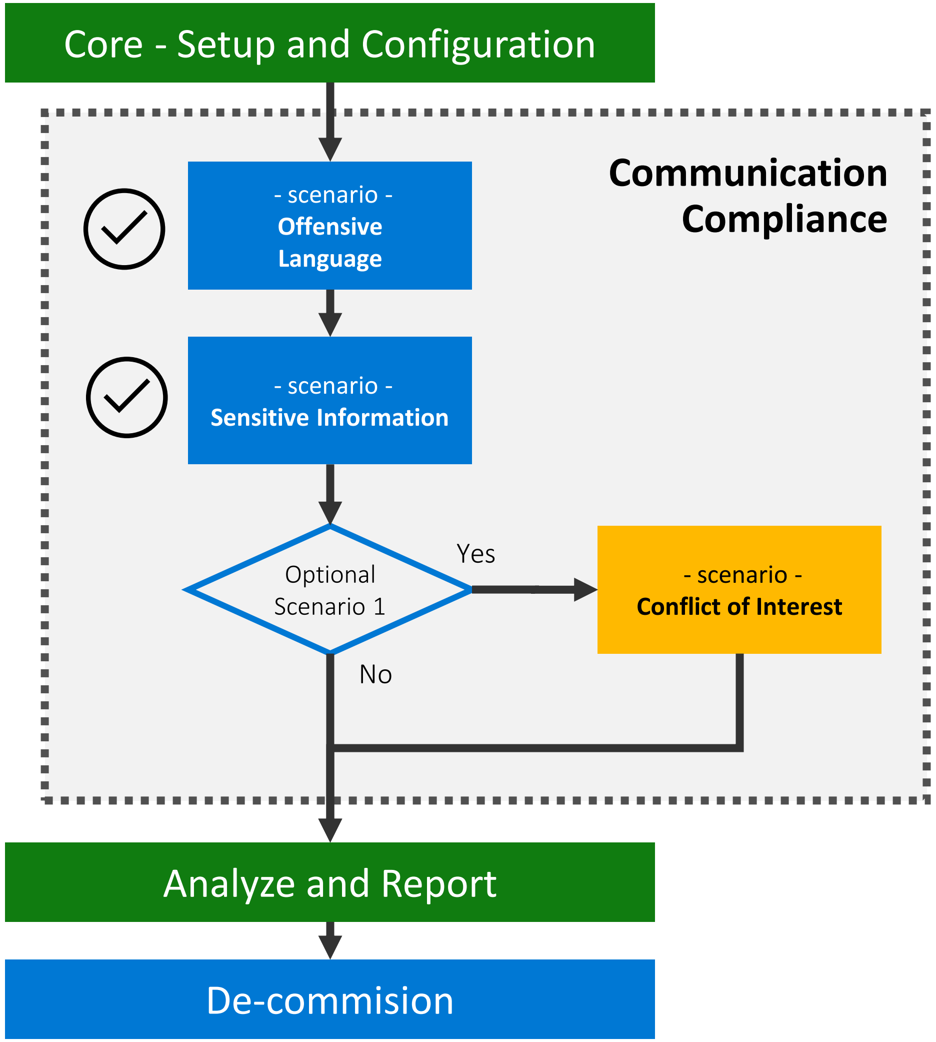
Detect communication risks in the organization by enabling Communication Compliance and configuring policies that will define the types of inappropriate content to identify and detect.

This activity covers:

- Offensive language
- Sensitive information

You can add an optional scenario:

- Conflict of interest


Core - Setup and Configuration
Communication Compliance
- scenario - Offensive Language
- scenario - Sensitive Information
Optional Scenario 1
Yes
No
- scenario - Conflict of Interest
Analyze and Report
De-commision

Exelegent

Sensitive information

Module - Communication Compliance

Monitor communications for sensitive information

- Exchange Online, Microsoft Teams, Yammer, Skype for Business
- Inbound, outbound, or internal only
- Review 10% of communications
- Sensitive information, out-of-the-box content patterns and types, custom dictionary option, attachments larger than 1 MB

Monitoring legitimate communications between employees, or between employees and outside parties

Data theft with malicious intent

Compliance Manager Tenant Assessment

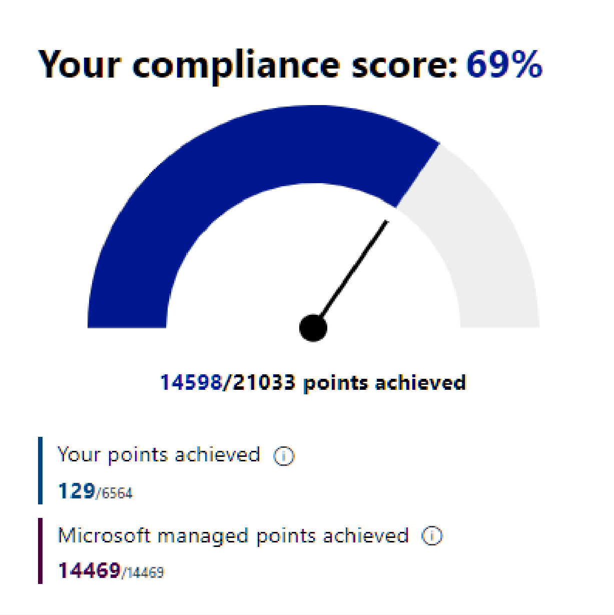
Assess performance relative to key data protection standards and regulations.

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.

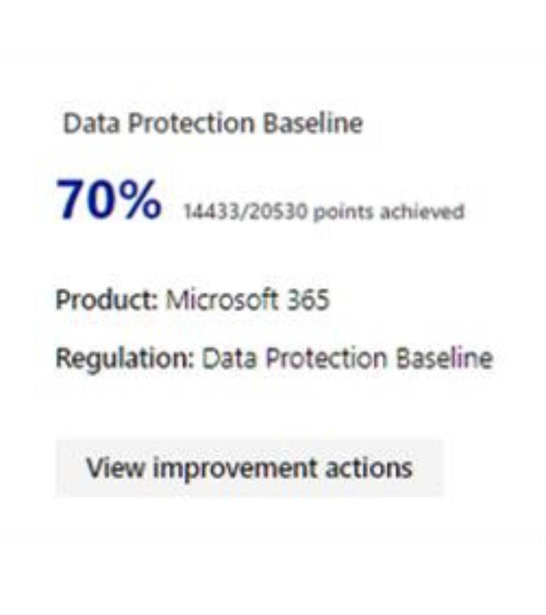


Your compliance score: 69%

14598/21033 points achieved

Your points achieved ⓘ
129/6564

Microsoft managed points achieved ⓘ
14469/14469

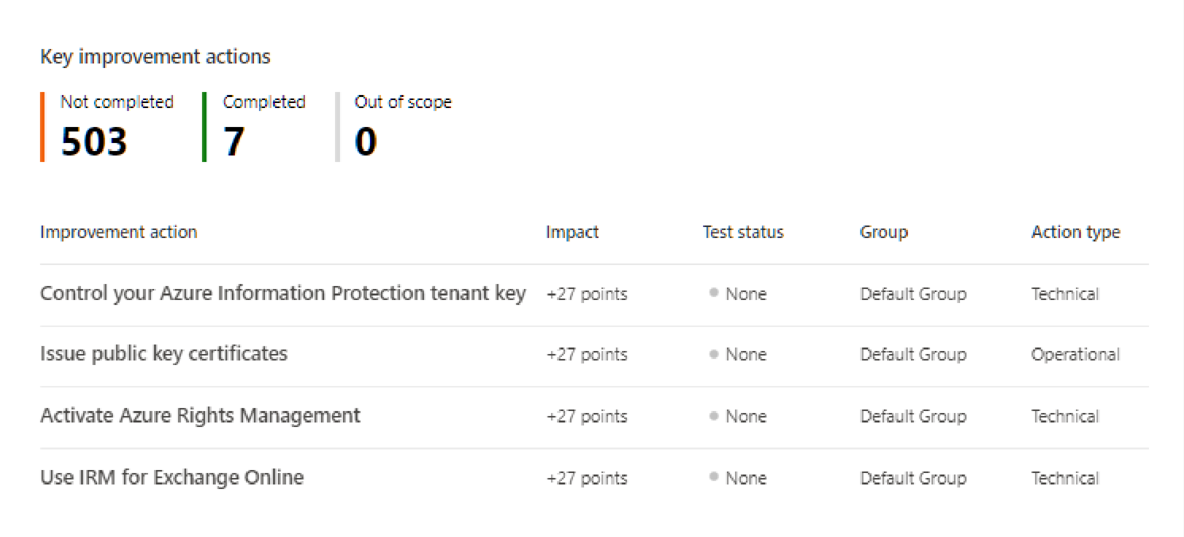


Data Protection Baseline

70% 14433/20530 points achieved

Product: Microsoft 365

Regulation: Data Protection Baseline

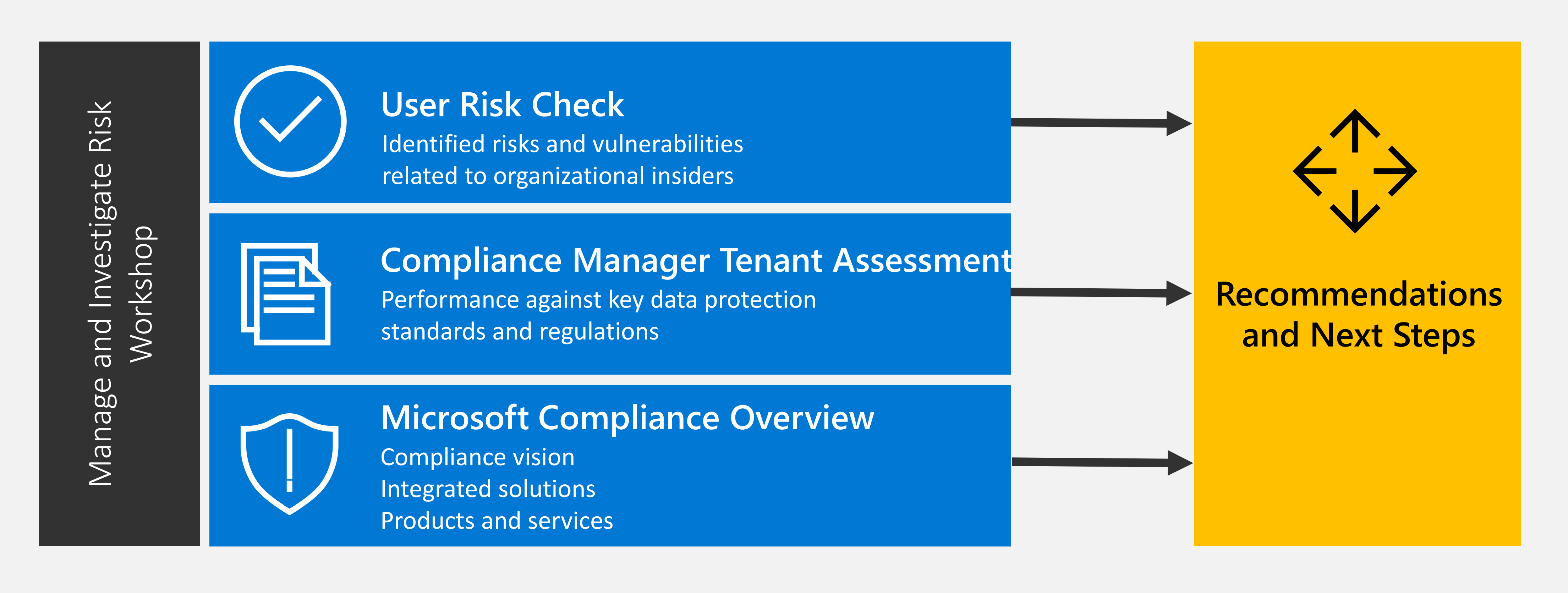


Key improvement actions

Not completed	Completed	Out of scope
503	7	0

Improvement action	Impact	Test status	Group	Action type
Control your Azure Information Protection tenant key	+27 points	● None	Default Group	Technical
Issue public key certificates	+27 points	● None	Default Group	Operational
Activate Azure Rights Management	+27 points	● None	Default Group	Technical
Use IRM for Exchange Online	+27 points	● None	Default Group	Technical

Recommendations and next steps



Manage and Investigate Risk Workshop

User Risk Check

Identified risks and vulnerabilities related to organizational insiders

Compliance Manager Tenant Assessment

Performance against key data protection standards and regulations

Microsoft Compliance Overview

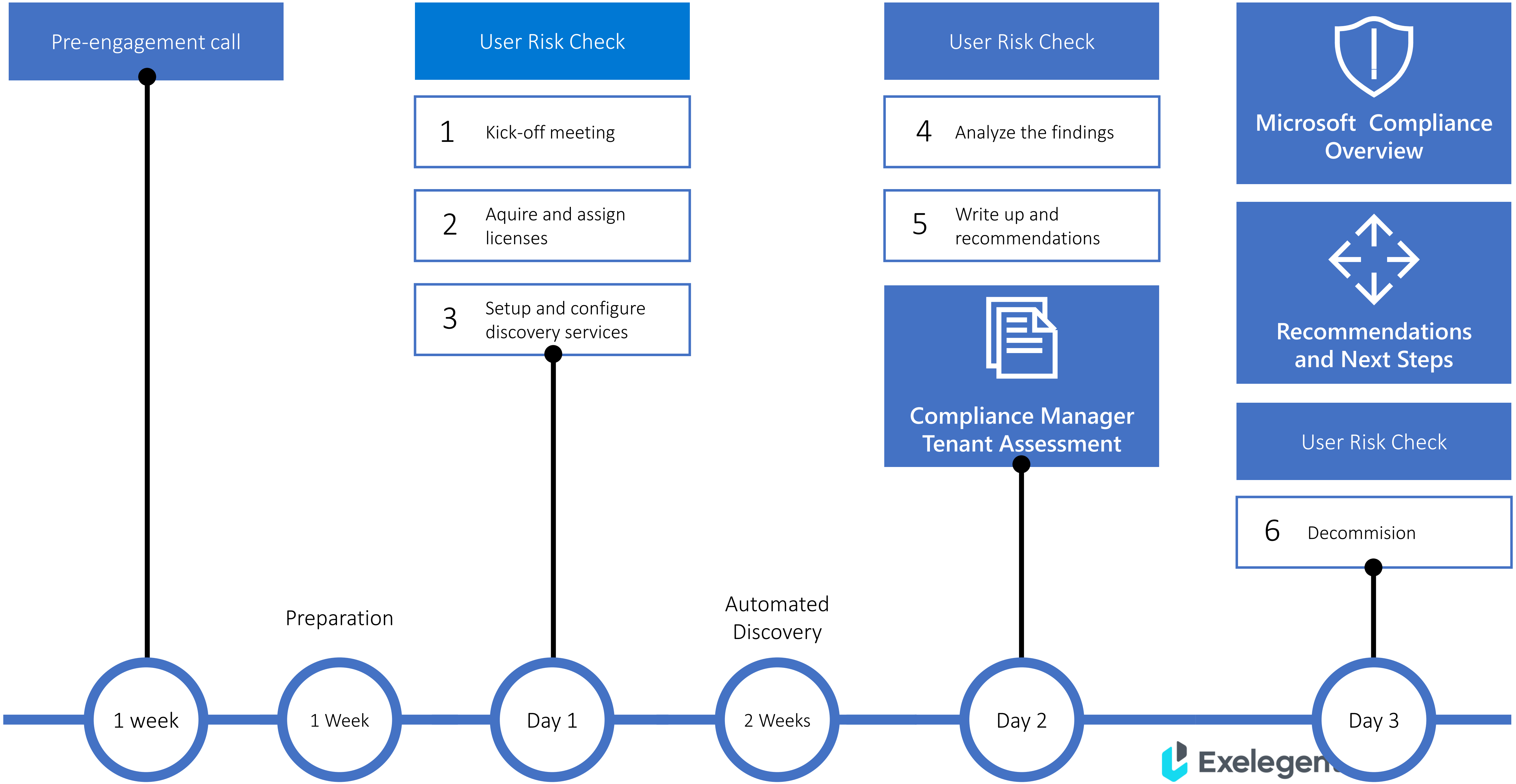
Compliance vision

Integrated solutions

Products and services

Recommendations and Next Steps

Workshop timeline



Pre-engagement call

User Risk Check

1 Kick-off meeting

2 Aquire and assign licenses

3 Setup and configure discovery services

User Risk Check

4 Analyze the findings

5 Write up and recommendations

Compliance Manager Tenant Assessment

Microsoft Compliance Overview

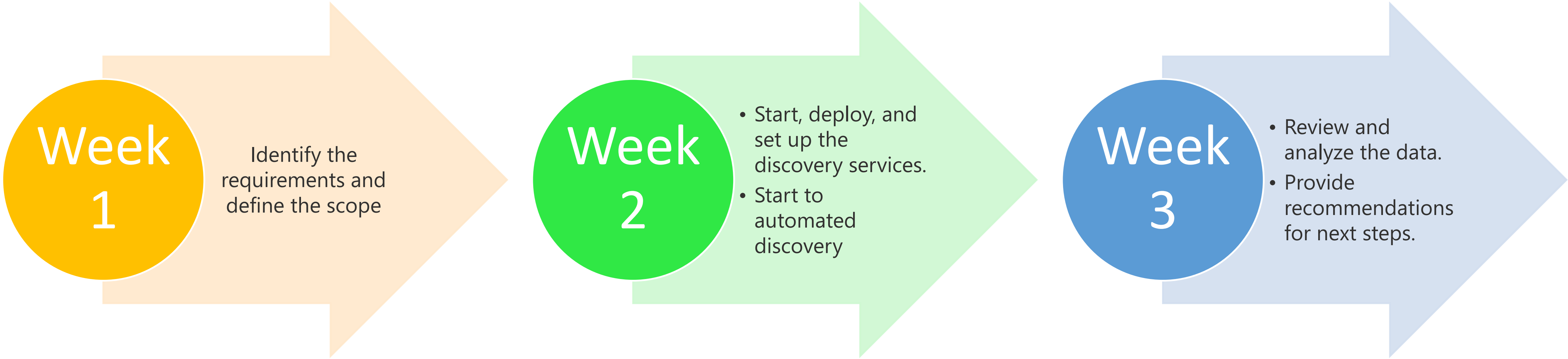
Recommendations and Next Steps

User Risk Check

6 Decommision

Exelegent

Weekly Agenda



Week 1

Identify the requirements and define the scope

Week 2

- Start, deploy, and set up the discovery services.
- Start to automated discovery

Week 3

- Review and analyze the data.
- Provide recommendations for next steps.