Data is exploding
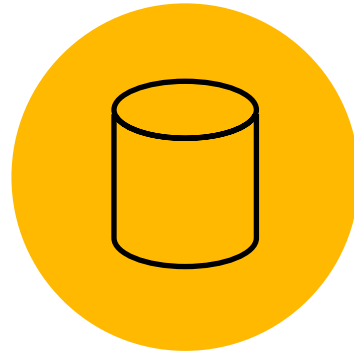
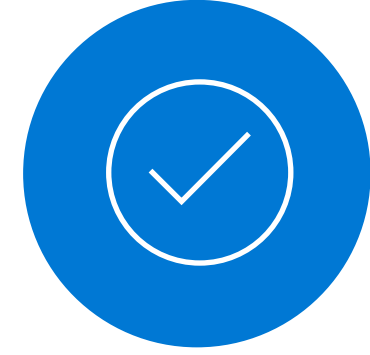It's created, stored, and shared everywhere
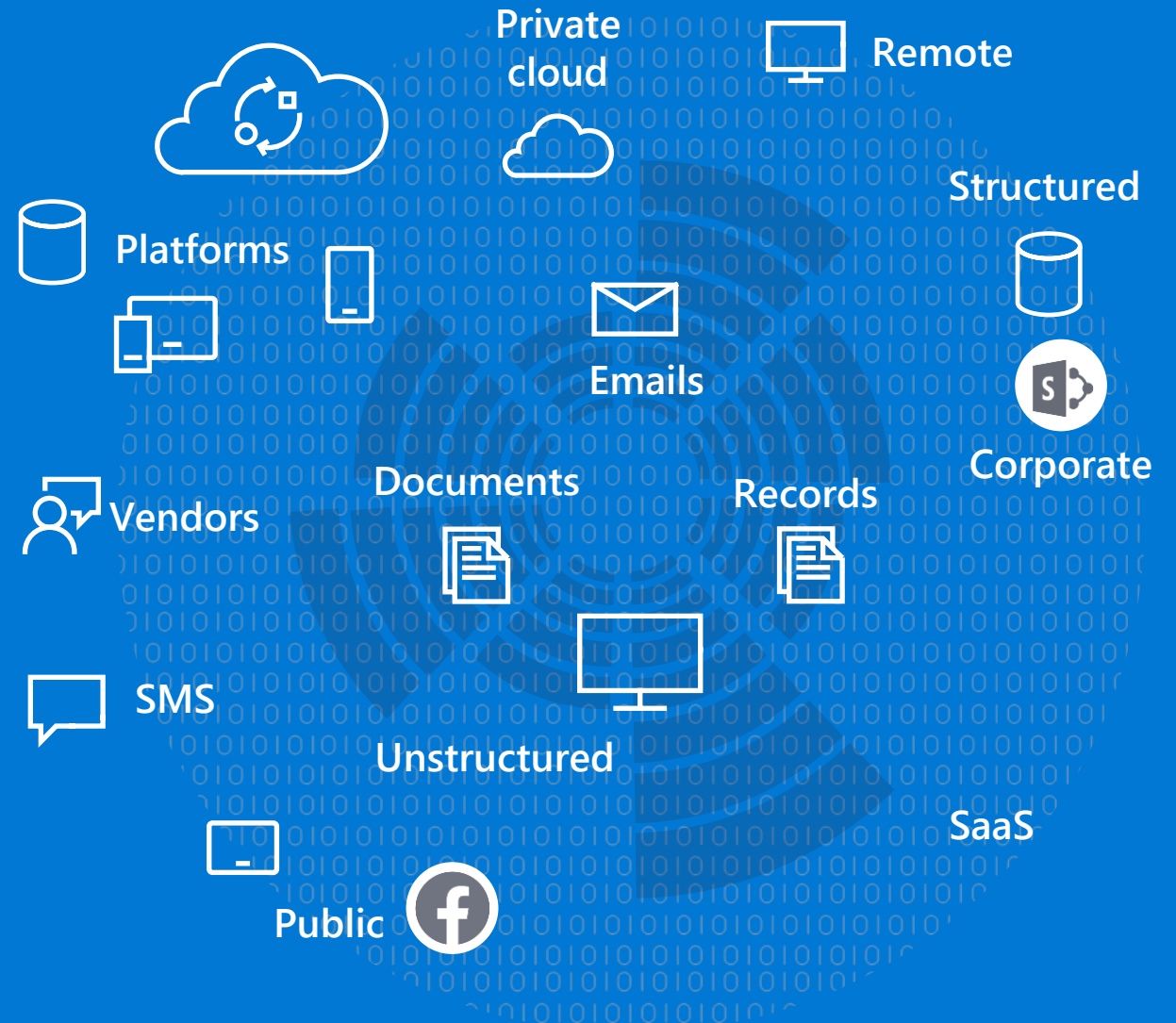
Discovering and managing data is challenging

88% of organizations no longer have confidence to detect and prevent loss of sensitive data[1]

>80% of corporate data is "dark" – it's not classified, protected or governed[2]

83% of companies are experiencing challenges in ensuring regulatory and industry compliance from ineffective data management[3]

1. Forrester. Security Concerns, Approaches and Technology Adoption. December 2018
2. IBM. Future of Cognitive Computing. November 2015
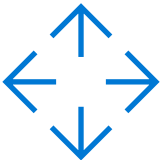3. Vanson Bourne. Realizing the Power of Enterprise Data. 2019.

Do you have a strategy for protecting and managing sensitive and business critical data?
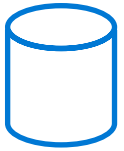
Do you know where your business critical and sensitive data resides and what is being done with it?

Do you have control of this data as it travels inside and outside of your organization?

Are you using multiple solutions to classify, label, and protect this data?

Data regulations are increasing around the world

|	
Personal Information Protection and Electronic Documents Act (PIPEDA)	General Data Protection Regulation (GDPR 2016)
California Consumer Privacy Act (CCPA) 2018	The Privacy Protection Act (PPA) 2017
Federal Data Protection Law 2000	Personal Data Protection Bill 2018
Texas Privacy Protection Act (2019)	Personal Data Protection Act (PDPA 2012)
Lei Geral de Proteção de Dados Pessoais (LGPD 2019)	Personal Information Security Specification 2018
Australia Privacy Principles 2014	Personal Information Protection Act (PIPA) 2011
Protection of Personal Information Act 2013 (POPI)	Act on Protection of Personal Information (APPI) 2017

The risks of not being compliant

Loss of trust

- Do customers still want to work with you if you lose their trust?

- Compliance as a basic requirement to do business.

Reputational damage

- Do you want to be the organization in the news?

- How would you like to be remembered?
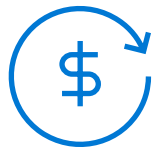
Fines

- Can be significant and are real.

Intelligent compliance and risk management solutions

Information Protection & Governance

Protect and govern data anywhere it lives

Internal Risk Management

Identify and remediate critical insider risks

Discover & Respond

Quickly investigate and respond with relevant data

Compliance Management | Simplify and automate risk assessments

What is the data risk check?

Automated Process that leverages Microsoft 365 services to look for customer relevant sensitive information that may impose a privacy or regulatory risk.
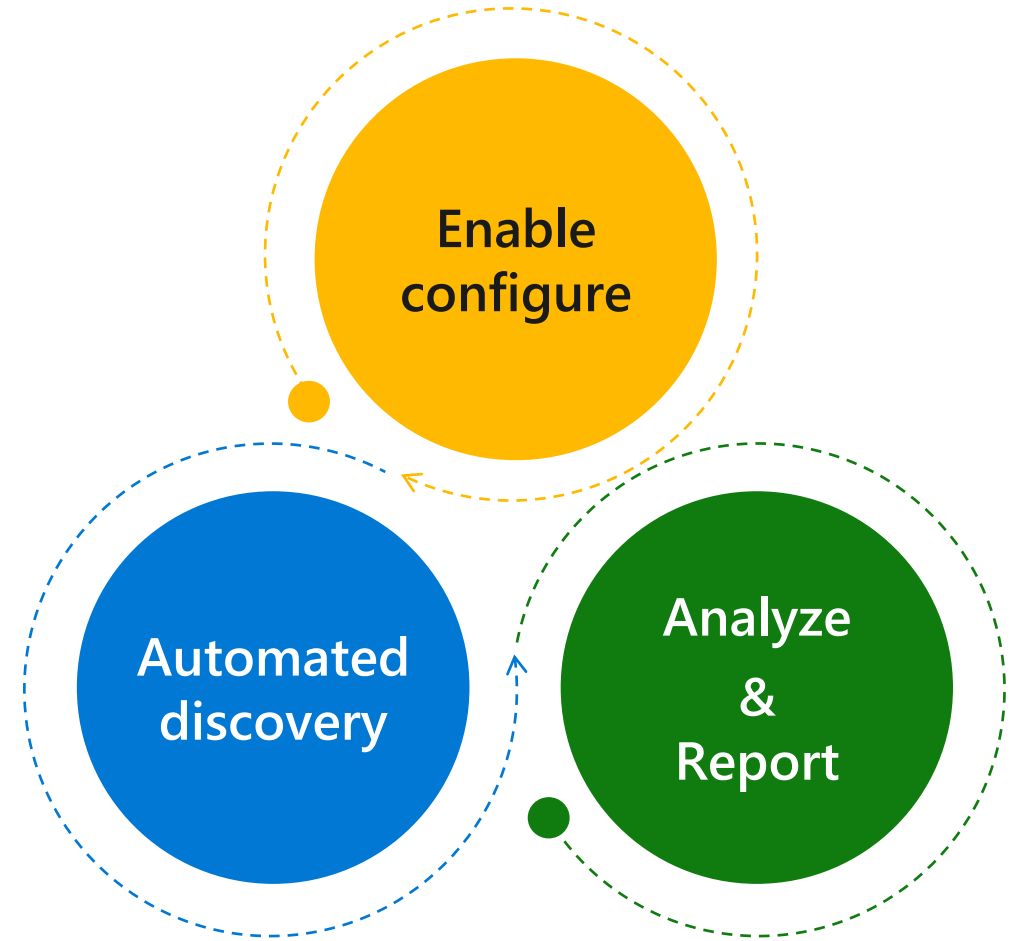
The Data Risk Check

Enable and Configure

Enable the services for **automated discovery, configure** the **search artifacts**

Automated Discovery

Two weeks of **automated discovery** searching for privacy and regulatory risks in organizational data

Analyze & Report

Analyze the findings and **report** on the identified privacy and regulatory risks.

What Auto Discovery looks for

Sensitive Information
Artifacts that are relevant to your organization and impose a privacy or regulatory risk.

Stale Data
E-mails, documents that should have been deleted years ago

Risky activity
Copying sensitive data to endpoints, USB drives or other uncontrolled locations.

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 Drivers 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)

Customer-specific sensitive info types

🌐 **Business intellectual property**
Business plans, product designs, confidential projects
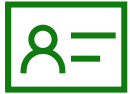
📇 **Employee or customer information**
HR Information, resumés, employment records, salary information

🔒 **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 choose 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

View improvement actions

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

How the Protect and Govern Sensitive Data Workshop can help

Understand the risks of *Dark Data*
Discuss and understand the hidden privacy and regulatory risks of dark data and how to mitigate.

Discover privacy and regulatory risks of existing data
Add insight into the organization's data across the organization.

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

Analyze and report
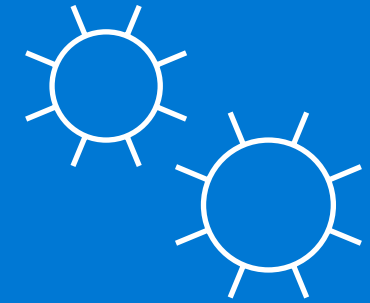Analyze the findings and associated privacy and regulatory risks. Provide insight and highlight most impactful.

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

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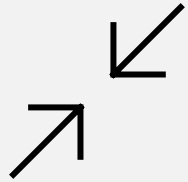Provide recommendations for risk mitigation and define actionable next steps

Engagement Objectives

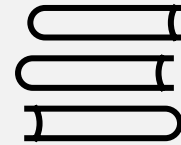**Protect and Govern Sensitive Data Workshop**
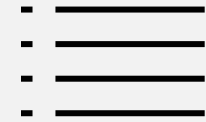
What we'll do during the workshop

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

Discover data risks in your environment across email, file storage, and use of data.

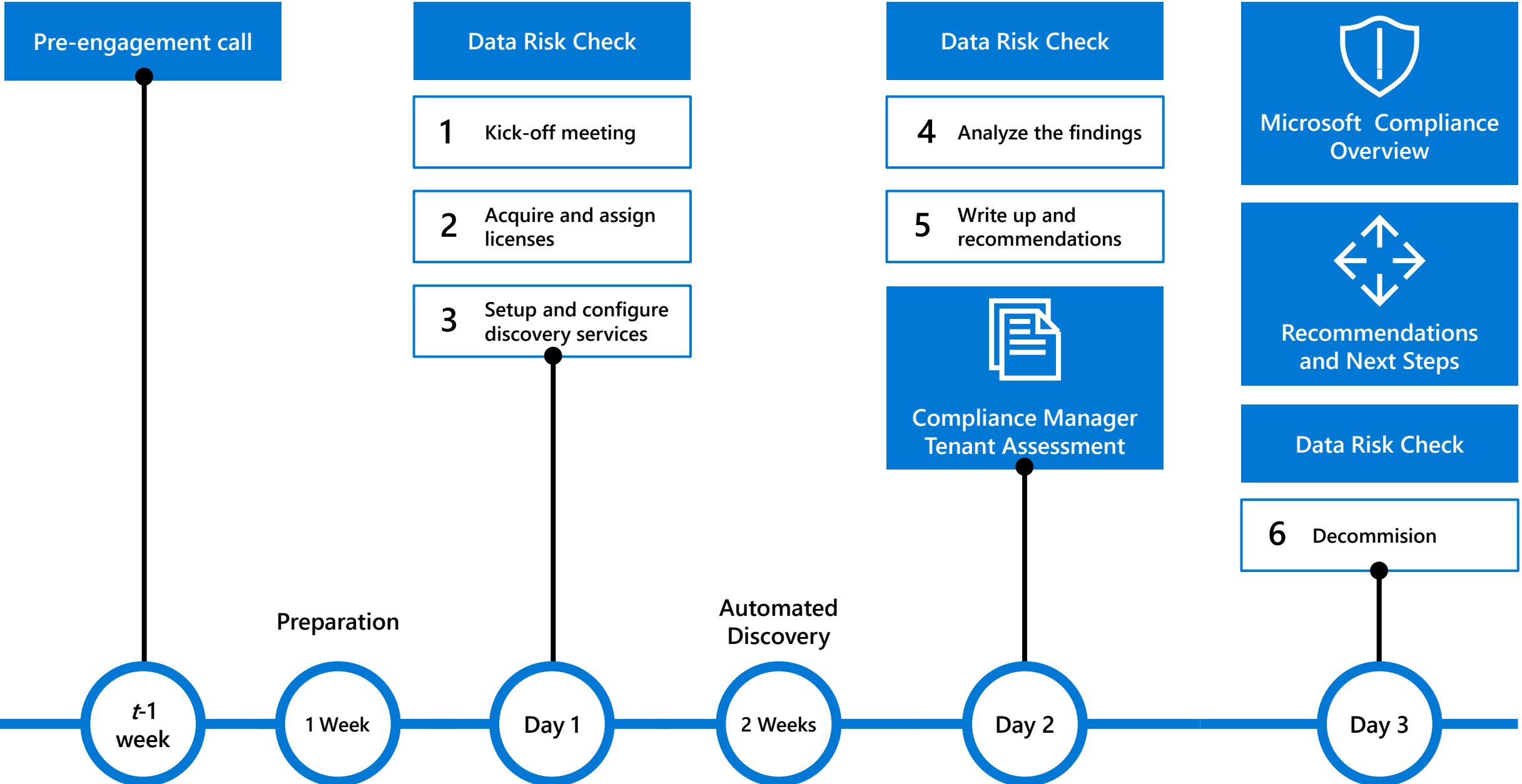Learn about Microsoft's approach to compliance with an immersive experience.

Plan next steps on how we can work together.

After the Workshop, you'll...

- Have compliance strategy documentation for your teams and stakeholders

- Better understand, prioritize, and mitigate potential threats

- Accelerate your compliance journey with Microsoft

- Have defined next steps based on your needs and objectives

Workshop timeline

Pre-engagement call

Data Risk Check

1	Kick-off meeting

2	Acquire and assign licenses

3	Setup and configure discovery services

Data Risk Check

4	Analyze the findings

5	Write up and recommendations

Compliance Manager Tenant Assessment

Microsoft Compliance Overview

Recommendations and Next Steps

Data Risk Check

6	Decommision

Preparation

Automated Discovery

t-1 week

1 Week

Day 1

2 Weeks

Day 2

Day 3

Q&A

Microsoft Security

Thank you

real impact

TECHNOLOGY CONSULTING