

Turn Compliance Stress into Compliance Success!



Mark Warnes, Kocho
Mark Dennis, Evolve North
Nathan Aldridge, Microsoft
Cristina Cuciula, Microsoft



Compliance drivers



Statutory and Industry Regulations

GDPR, Data Protection Act 2018, Misuse of Computers Act, Privacy Regulations, ePrivacy, NIST, PCI DSS, Cyber Essentials, ISO27001, DSP Toolkit, FCA, ICO – **we operate in a regulated environment**

DPO/Compliance

Corporate policies and processes, internal/external audit, ongoing assurance, training and education, breach/incident management, Subject Access Requests – **we need as much visibility as possible**

Your users

Content creators, data handlers/processors, sharing content (sometimes passwords) working collaboratively, home working, multi organisation working – **we need to help users as much as we can**

Your Board

Your Board and Senior Management Team need to be confident that they are operating a compliant and safe business model that is fit for purpose – **we need to provide that assurance**

We need to exploit all the tools we have at our disposal to manage the above

GDPR Sunset



Government Statement

The UK Government has stated it will "sunset" the GDPR by 2023 – this is in advance of the current GDPR Adequacy agreement which expires in 2025 – this provides significant challenges – globally not just EU

The Great British Data Protection Act

UK Government will need to create a new Data Protection Act, agree its adequacy with the EU, get it into UK law, have it deployed into UK business – all within 15 months.....

If we don't achieve this?

Implications could be – legal data sharing agreements, standard contractual clauses, corporate binding rules, external audit. Will we need ISO27001, NIST Audits? To continue doing business.

What could happen?

The current adequacy agreement stays in place until 2025 as delivering the GBDPA and an adequacy agreement is probably not achievable in 15 months.... however, it makes sense to identify and manage this risk.

We need to exploit all the tools we have at our disposal to manage the above

Why bother?



Cost

When data protection fails it is never cheap to fix, the cost of successful Ransomware/Breach is staggering to rectify and often Cyber Insurance will not cover it – **it is cheaper to address the challenge – identify risk and manage it**

Reputation

Reputational damage and the associated loss/cost to the business will always be substantial particularly if the ICO prosecutes you for negligence – **ensure you are not negligent - risk management keeps you safe**

Staff impact

Do not underestimate the impact on staff if this goes wrong, particularly if they are a good person making a simple mistake on a simple transaction – **we need to protect users as much as we can – we are all data subjects**

Data Subjects

We have a legal responsibility to look after the data and the rights of all data subjects including clients, staff, board members, the general public – **we need to meet our responsibilities – its good business practice**

It always costs more to fix than to maintain.



Information Protection and Governance

Safeguard sensitive data across clouds, apps and endpoints.

Supports:

- GDPR
- Data Protection Act
- PCI DSS
- FCA Regulation
- DSP Toolkit
- Cyber Essentials
- ISO 27001

Protects the end user and your data

Risk Management

Identify and remediate critical risks within your organisation.

Provides:

- Templates
- Reports
- Alerts & Notifications
- Audit trails
- Standard Metrics
- Visibility & Control
- Assurance

Risk reduction

Compliance Management

Assess compliance and respond to regulatory requirements.

Delivers:

- Compliance visibility
- Assurance to the Board, external auditors, and all stakeholders
- Provides comparable metrics (e.g. NIST)
- Involves the whole business

Protects the business, your staff, and your clients



Information Protection and Governance



Data Classification

Know what types of data you have, where it resides, and what is happening to it



Information protection

Classify and protect files and messages with sensitivity labels and portable encryption



Data Loss Prevention

Protect sensitive information from risky access across apps, services and endpoints



Data Lifecycle Management

Govern your data at scale with flexible policies and labels for retention and/or deletion



Records Management

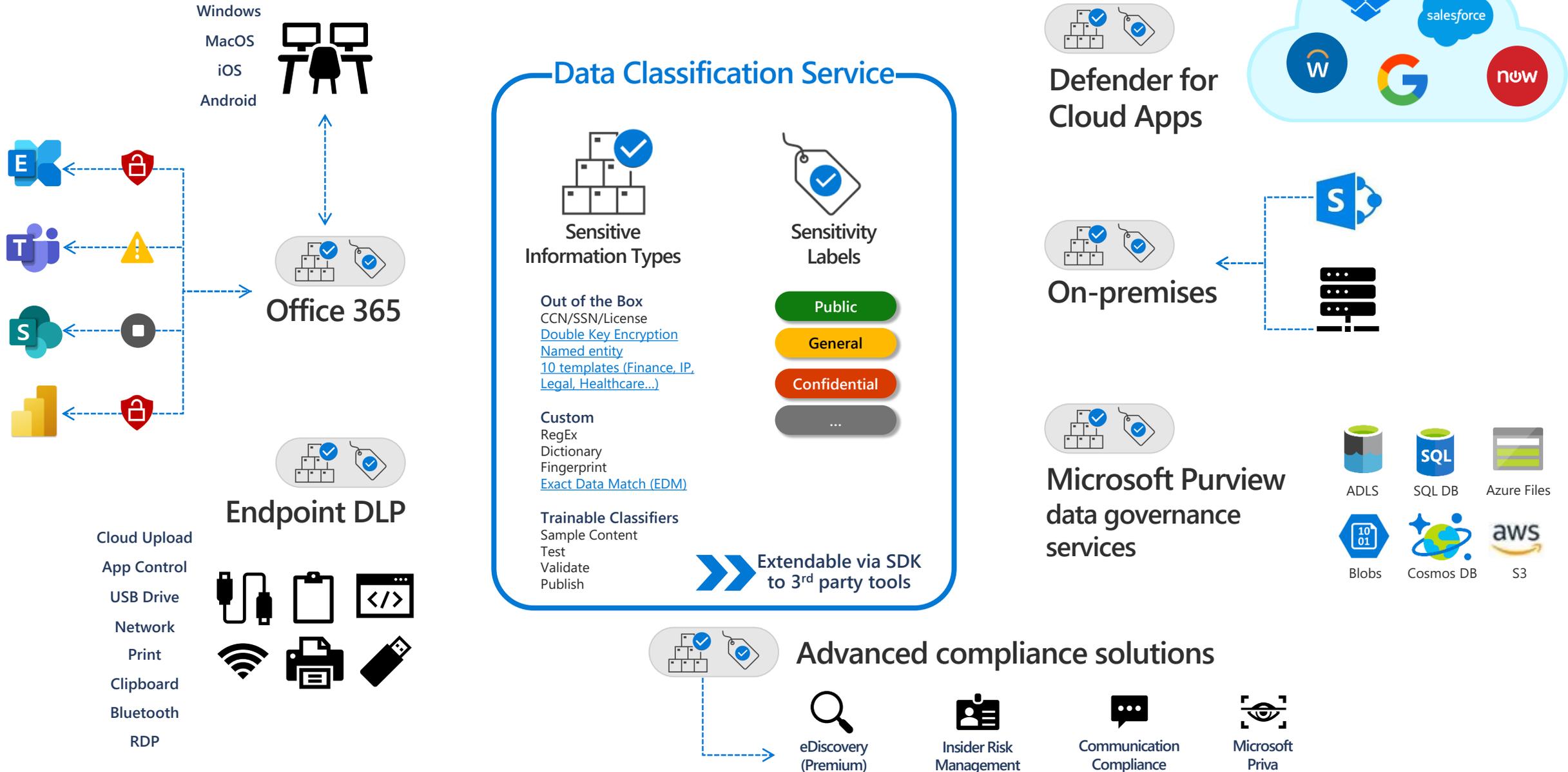
Govern your critical records with a central file plan, audited disposals and reviews



Data Map and Data Catalog

Discover and visualize data from hybrid sources, manage metadata, and maximise value

Microsoft Purview Information Protection





Demo

Information Protection
and Governance

Data classification

Overview Trainable classifiers Sensitive info types Content explorer Activity explorer

Get snapshots of how sensitive info and labels are being used across your organization's locations. [Learn more](#)

Top sensitive info types

Sensitive info types used most in your content



[View all sensitive info types](#)

Azure Information Protection labels summary

No audit data exists

[Go to AIP portal](#)

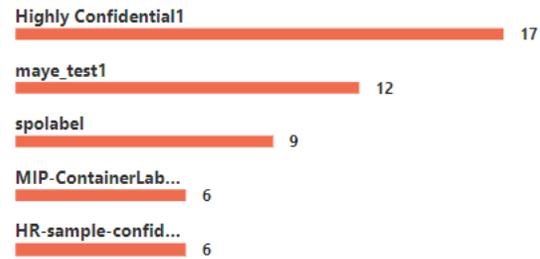
Top activities detected

83033 activities

59.3K File created
15.4K File modified
6.2K File copied to network share

[View all activities](#)

Top sensitivity labels applied to content



[View all applied sensitivity labels](#)

Top retention labels applied to content



[View all applied retention labels](#)

Locations where sensitivity labels are applied



[View details](#)

Locations where retention labels are applied



[View details](#)

File Home Insert Draw Design Layout References Mailings Review View Help

Undo Paste Copy Format Painter Clipboard Font Paragraph Styles

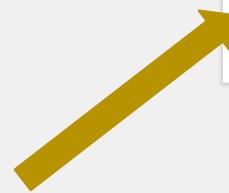
Normal No Spacing Heading 1 Heading 2 Title Subtitle Subtle Emphasis

Find Replace Select Editing Dictate Voice

Sensitivity Editor Reuse Files

admin@M365x02473751.onmicrosoft.com

- Personal
- Public
- General >
- Confidential >
- ✓ Highly Confidential >

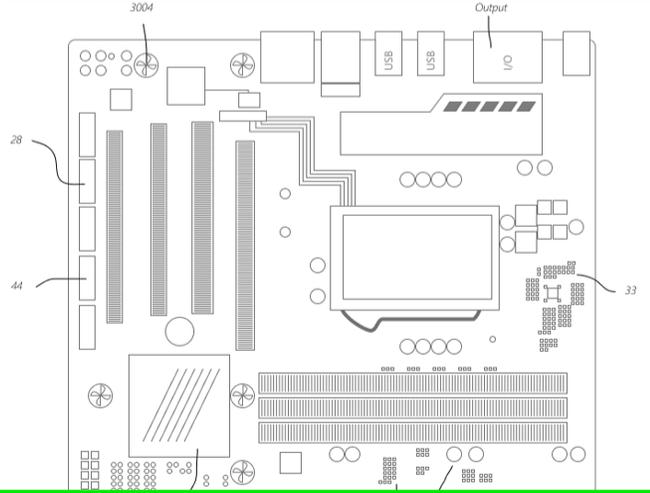


Project Obsidian

Updated Engine Chip Design

Automated Car Team
Feb 4, 2022

Contacts	Email	Timeline
Lidia Holloway	lidia@contosoelectronics.com	Q4 FY 22



Built-in: End user manual labeling in Office apps across Windows, Mac, iOS, and Android

Excel

Confidential... MOD Administrator

File name: Confidential Customer List.xlsx

Location: 02-Confidential
Contoso » Shared Documents » Seed data

Version History

Sensitivity: admin@M365x02473751.onmicrosoft.com

- Personal
- Public
- General
- ✓ Confidential
- Highly Confidential

	C	D	E	F
Muhammed MacIntyre	3	-213.25	38.94	
Barry French	293	457.81	208.16	
Barry French	293	46.71	8.69	
Clay Rozendal	483	1198.97	195.99	
Carlos Soltero	515	30.94	21.78	
Carlos Soltero	515	4.43	6.64	
Carl Jackson	613	-54.04	7.3	
Carl Jackson	613	127.70	42.76	
Monica Federle	643	-695.26	138.14	
Dorothy Badders	678	-226.36	4.98	
Neola Schneider	807	-166.85	4.28	
Neola Schneider	807	-14.33	3.95	
Carlos Daly	868	134.72	21.78	
Carlos Daly	868	114.46	47.98	
Claudia Miner	933	-4.72	5.28	
Neola Schneider	995	782.01	20.80	

Mobile

Contoso Confidential. Sensitive business data that

M&A Plan –

January 2019, CONTOSO I
M&A ID: #CO0151500

An M&A proposal regarding the potential
“Shanghai.” Prepared by the Contoso Merg
department at Contoso, Colorado during Q
Colorado - 319 W. 4th Street, P.O. Box 123
555-1234

www.contosowater.org

Sensitivity

- Public
- General
- Confidential
- Highly Confidential
- Learn More...

Outlook & OWA

U.S. Sales

Private group • 7 members

Sensitivity: Confiden

- Personal
- Public
- General
- ✓ Confidential
- Highly Confidential

Anyone (unrestricted)

All Employees

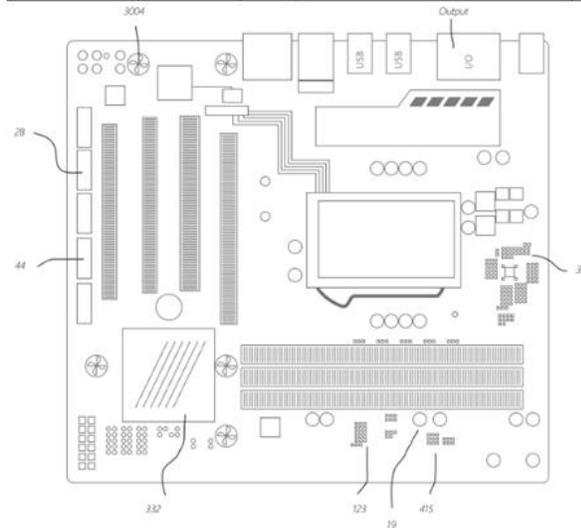
Unified & Built-in: Native labeling across all apps and modalities

Project Obsidian

Updated Engine Chip Design

Automated Car Team
October 21, 2019

Contacts	Email	Timeline
Lidia Holloway	lidia@contosoelectronics.com	Q4 FY 22

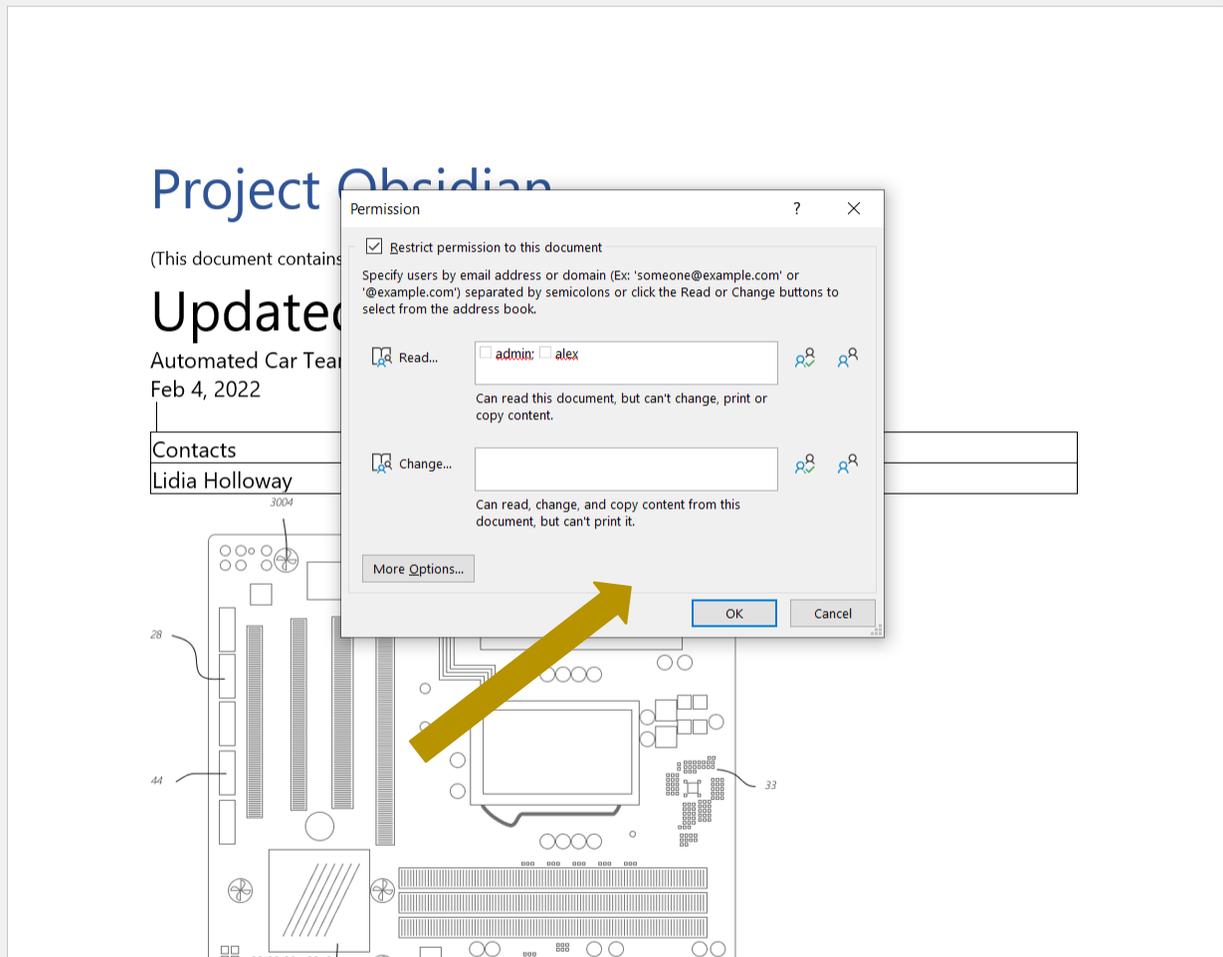


With our new investments in automated cars we need to redesign the AI500 chip to pull more throughput and reduce overheating.

Auto-labeling in Office Apps

credit card information:

Visa: 4538-1978-4719-4203 Exp: 08/2023



Built-in: User defined permissions when applying label



- Choose the information to protect**
- Name your policy
- Locations to apply the policy
- Policy settings
- Test or turn on the policy
- Review your settings

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. [Learn more about DLP policy templates](#)

- ### Categories
- Financial
 - Medical and health
 - Privacy
 - Custom**

- ### Templates
- Custom policy**

Custom policy

Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.

Next

Cancel



- Choose the information to protect
- Name your policy
- Locations to apply the policy**
- Policy settings
- Test or turn on the policy
- Review your settings

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

i Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> On	Exchange email	All Choose distribution group	None Exclude distribution group
<input checked="" type="checkbox"/> On	SharePoint sites	All Choose sites	None Exclude sites
<input checked="" type="checkbox"/> On	OneDrive accounts	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	Teams chat and channel messages	All Choose account or distribution group	None Exclude account or distribution group
<input checked="" type="checkbox"/> On	Devices	All Choose user or group	None Exclude user or group
<input checked="" type="checkbox"/> On	Microsoft Defender for Cloud Apps	All Choose instance	None Exclude instance
<input checked="" type="checkbox"/> On	On-premises repositories	All Choose repositories	None Exclude repositories
<input type="checkbox"/> Off	Power BI (preview)		

Data loss prevention > Create policy

Choose the information to protect

Name your policy

Locations to apply the policy

Policy settings

Info to protect

Protection actions

Customize access and override settings

Test or turn on the policy

Review your settings

Audit or restrict activities on Windows devices

When the activities below are detected on Windows devices for supported files (Word, PowerPoint, Excel, .pdf, .csv, and .txt) containing sensitive info that matches this policy's conditions, you can choose to only audit the activity, block it entirely, or block it but allow users to override the restriction. [Learn more](#)

- Upload to cloud services or access by unallowed browsers
- Copy to clipboard
- Copy to a USB removable media
- Copy to a network share
- Access by unallowed apps
- Print

Restrict Third Party Apps

Use one of the automatic actions provided by Microsoft Cloud App Security. [Learn more](#)

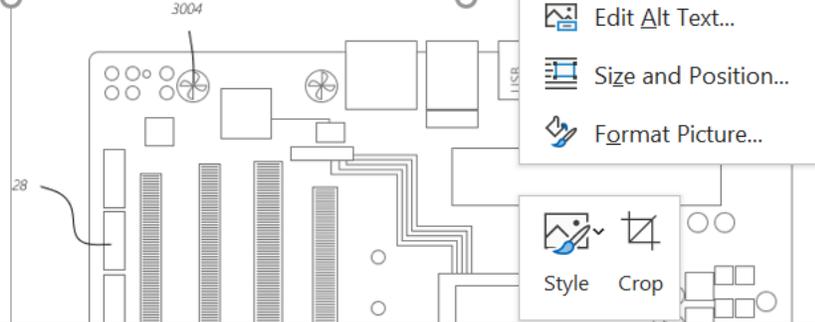
- Box**
 - Send policy-match digest to file owner
 - Remove external users
 - Trash file
 - Remove direct shared link
- G Suite**
 - Send policy-match digest to file owner
 - Make private
 - Remove external users
 - Trash file
- Cisco Webex**
 - Trash file
- Dropbox**

Project Obsidian

Updated Engine Design

Automated Car Team
October 21, 2019

Contacts	Email
Lidia Holloway	lidia@contos



- Cut
- Copy
- Paste Options:**
- Edit Picture
- Change Picture >
- Group >
- Bring to Front >
- Send to Back >
- Link >
- Save as Picture...
- Insert Caption...
- Wrap Text >
- Edit Alt Text...
- Size and Position...
- Format Picture...

- Style
- Crop

Data Loss Prevention

This action is blocked

You should not copy data while Project Obsidian Spec.docx is open. If you allow it you'll need to retry the copy.

Dismiss Allow



File Explorer window showing Desktop contents:

- Documents
- Pictures
- Captures
- Data
 - Customer Accounts Q4
 - Not Sensitive
 - Project Obsidian Spec
 - Project Obsidian
 - Project Omega
- Music
- Videos
- OneDrive - Person
- This PC
- TAKEHOME (D:)
- Network

Summary: 6 items, 3 items selected, 699 KB

Context menu: + Copy to TAKEHOME (D:)

1 Interrupted Action dialog box:

This action is blocked, but you can choose to allow it. Please refer to the data loss prevention notification for further information.

Project Obsidian
Type: Microsoft Edge PDF Document
Size: 618 KB
Date modified: 7/8/2020 7:50 PM

Do this for all current items

Buttons: Try Again, Skip, Cancel

More details

Size
247 KB
1 KB
67 KB
619 KB
15 KB

Data Loss Prevention

Your organization's policy
Saving to removable media with sensitive files open is not recommended. If you allow it, you'll need to resave.

Buttons: Dismiss, Take action

Your content was blocked because it has sensitive data

You're trying to use protected content in an unapproved website. Your approval is needed to share this content.

[Learn more](#)

Yes Cancel

Recycle Bin

Project Obsidi...

Project Obsidian

Home

Files

All files

Shared

File requests

Deleted files

Tools

Paper

Transfer

Showcase

Fabrikam
1 member

Recents Folders Files Links

Your shared folders and files will show up here so they're easy to find.

PDF

Proj + Copy
Obsidian

Create shared folder

Privacy ?



Risk Management



Insider risk management

Detect risky activity to identify, investigate, and take action on insider risks and threats



Communication compliance

Capture inappropriate messages, investigate policy violations, and remediate risks



Information barriers

Prevent conflict of interest and enable business separation between user groups



eDiscovery

Identify, preserve, analyse, and export data in response to legal discovery requests



Audit

Record and investigate user and admin activity across all locations and services



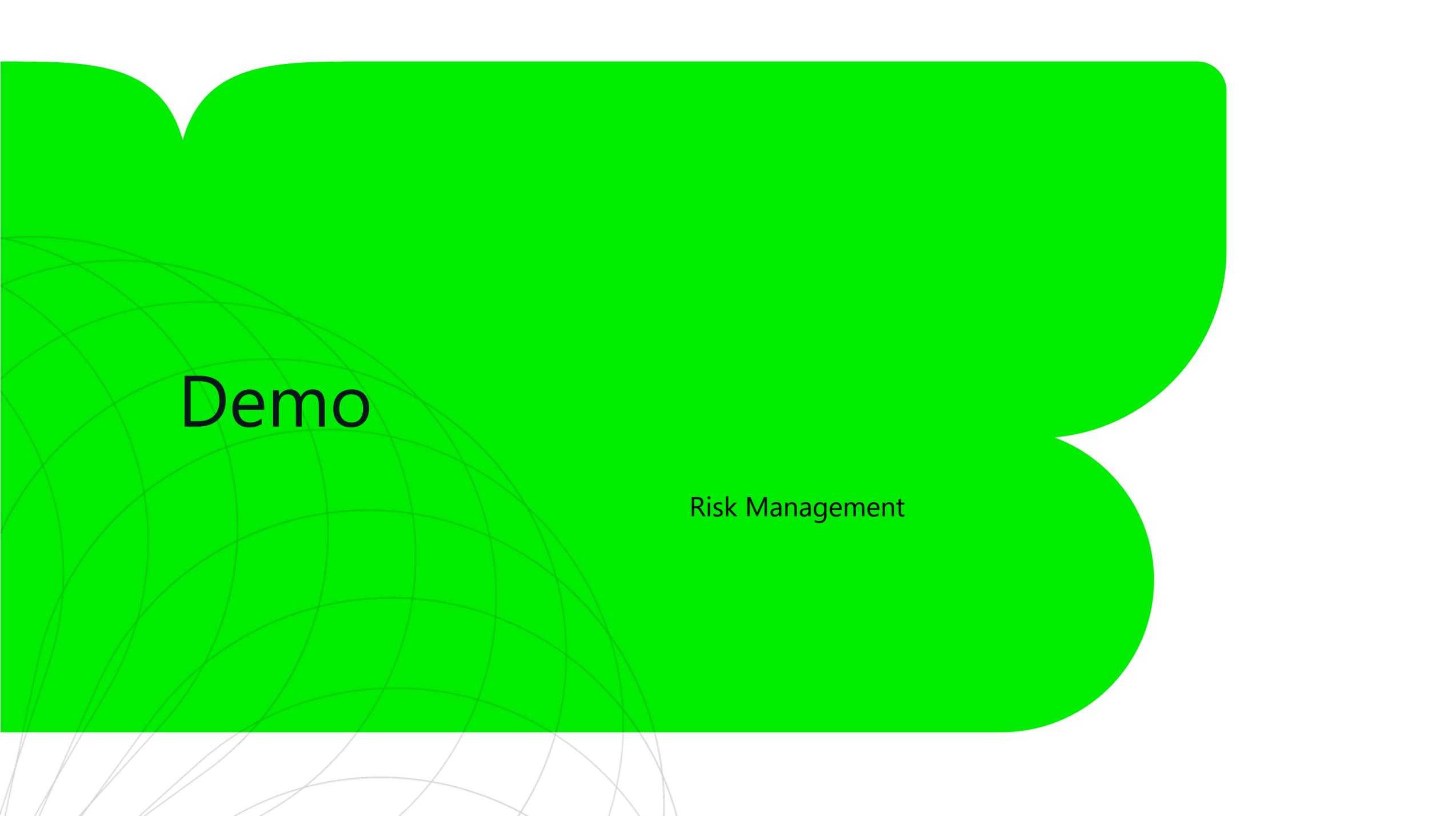
Privileged access management

Approve and escalate admin roles when required and eliminate standing access



Customer lockbox

Provide just-in-time access to your environment for Microsoft Support engineers



Demo

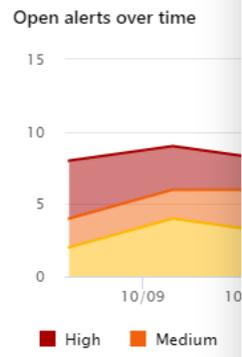
Risk Management

- Home
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
- Catalog
- More resources

Insider risk management

Overview Alerts Cases Policies Users Notices

Alerts needing review
3 alerts need review
3 alerts need review with no open cases



Export

Alert	Status	Severity	Age	Action
Policy match alert				
Anony85KF-34DF (1)				
Alert: Confidentiality obligation during departure	Needs review	High		<input checked="" type="radio"/>
AnonyO4J5-34PP (1)				
Alert: Project Jupiter Confidentiality	Needs review	Medium	2 years ago	<input type="radio"/>
AnonyF3FD-34PK (1)				
Alert: Anti-harrasment policy	Needs review	Low	2 years ago	<input type="radio"/>
AnonyIS8-978 (1)				
Alert: Confidentiality obligation during departure	Confirmed	High	a month ago	<input type="radio"/>

Alert: Confidentiality obligation during departure

Overview **User activity** User profile

History of recent user activity

- 09/16/2019
HR Event: Resignation Date Set
Resignation date set for: 09/27/2019
- 09/15/2019
File(s) printed
Risk Score: 65
10 file(s) were printed
4 file(s) have labels including: Top Secret
- 09/15/2019
File(s) copied to USB device
Risk Score: 92
113 file(s) were copied to USB device(s)
54 file(s) have labels including: Top Secret
- 09/15/2019
File(s) downloaded from SharePoint Online
Risk Score: 34
113 file(s) were downloaded from 1 SharePoint Online site(s)
54 file(s) have labels including: Top Secret

[Confirm and create new case](#) [Dismiss as benign](#)

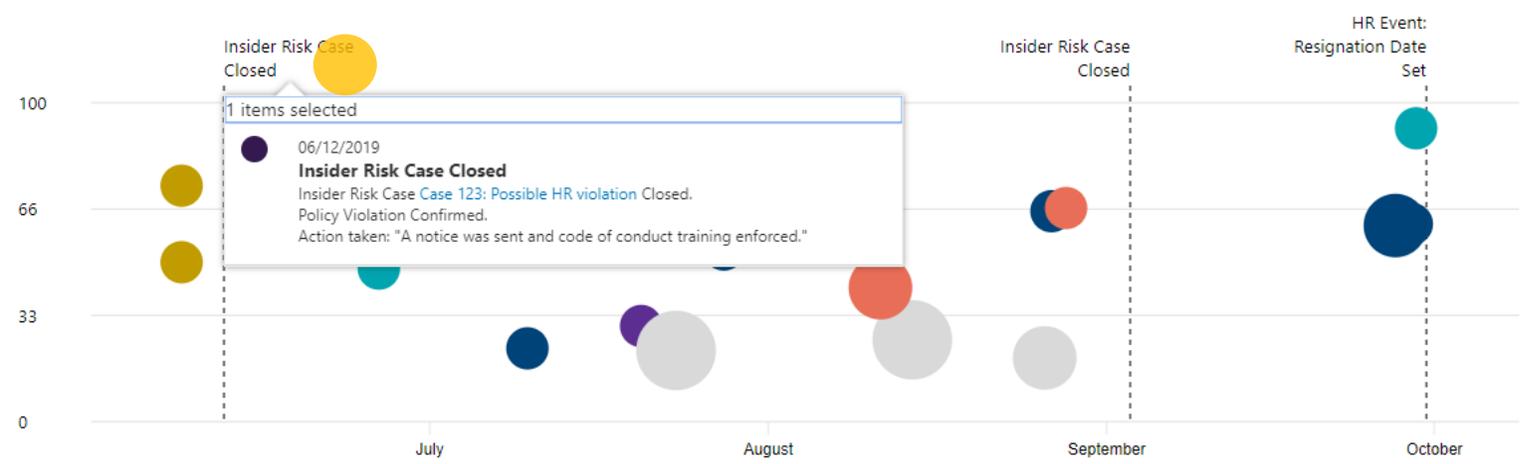
Case > IP Theft case

Pseudonymize On Open investigation Send e-mail notice Resolve case

Case overview Alerts User activity Content explorer Social graph Case notes Contributors

Export

04/24/2019 - 10/24/2019 25 risky activities Filter



- Shared from SharePoint Online
- File(s) copied
- File(s) printed
- Email(s) sent externally
- Security tampering or harmful software
- Offensive language detected
- Others
- Compound

09/30/2019
HR Event: Resignation Date Set
 Resignation date set for: 10/11/2019

Case details User details

About this case

Case name
IP Theft case

Case status
Active

Current risk level



Alerts confirmed
 Alert: Confidentiality obligation during departure

Need help? Feedback

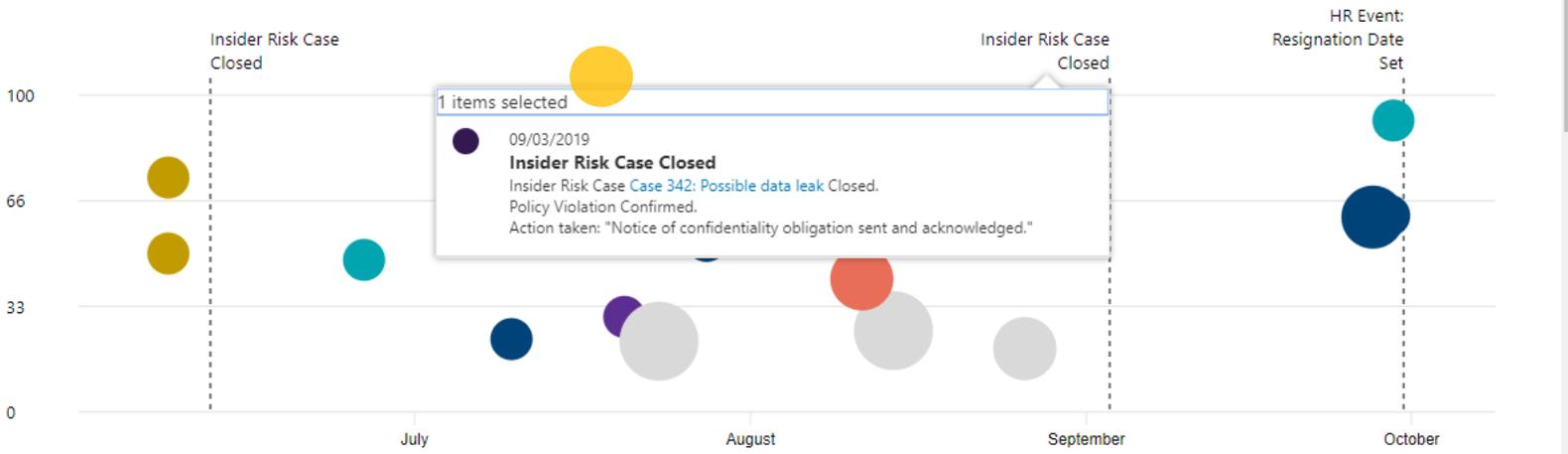
Case > IP Theft case

Pseudonymize On Open investigation Send e-mail notice Resolve case

Case overview Alerts User activity Content explorer Social graph Case notes Contributors

Export

04/24/2019 - 10/24/2019 25 risky activities Filter



- Shared from SharePoint Online
- File(s) copied
- File(s) printed
- Email(s) sent externally
- Security tampering or harmful software
- Offensive language detected
- Others
- Compound

09/30/2019
HR Event: Resignation Date Set
 Resignation date set for: 10/11/2019

Case details User details

About this case

Case name
IP Theft case

Case status
Active

Current risk level



Alerts confirmed
 Alert: Confidentiality obligation during departure

Need help? Feedback

- Home
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
- Catalog
- More resources

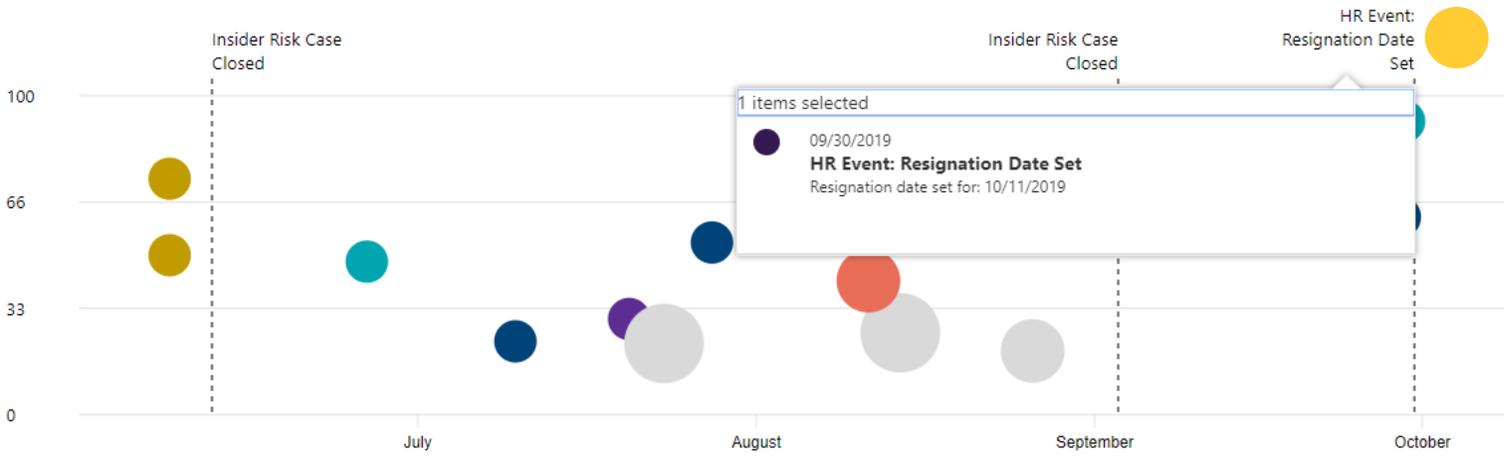
Case > IP Theft case

Pseudonymize On Open investigation Send e-mail notice Resolve case

Case overview Alerts User activity Content explorer Social graph Case notes Contributors

Export

04/24/2019 - 10/24/2019 25 risky activities Filter



- Shared from SharePoint Online
- File(s) copied
- File(s) printed
- Email(s) sent externally
- Security tampering or harmful software
- Offensive language detected
- Others
- Compound

09/30/2019
HR Event: Resignation Date Set
 Resignation date set for: 10/11/2019

Case details User details

About this case

Case name
IP Theft case

Case status
Active

Current risk level



Alerts confirmed
 Alert: Confidentiality obligation during departure

Need help? Feedback

- Home
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
- Catalog
- More resources

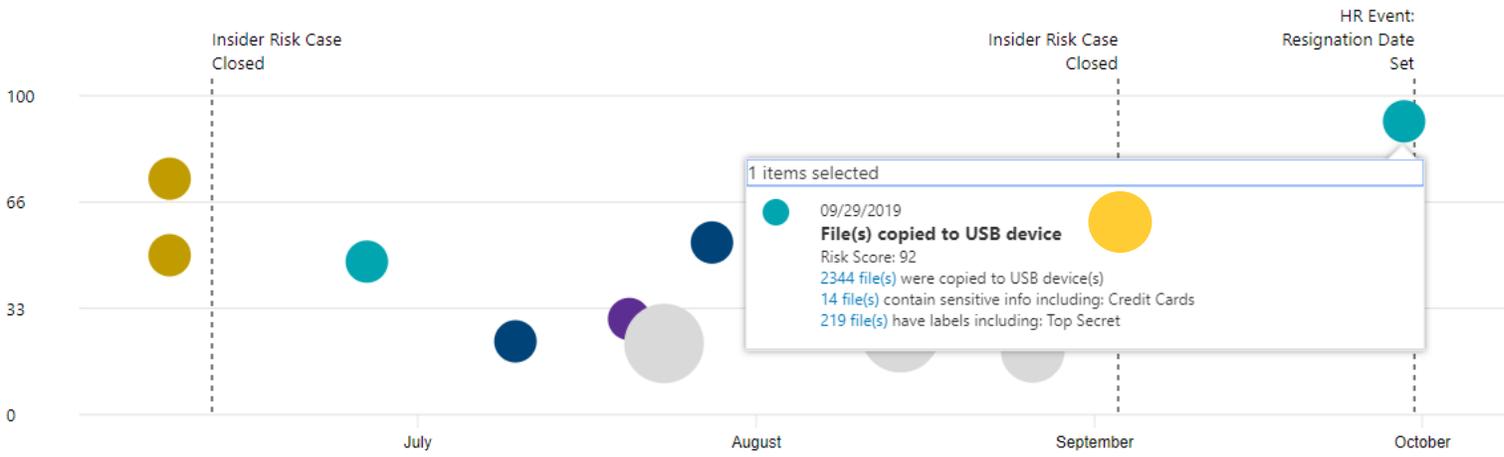
Case > IP Theft case

Pseudonymize On Open investigation Send e-mail notice Resolve case

- Case overview
- Alerts
- User activity**
- Content explorer
- Social graph
- Case notes
- Contributors

Export

04/24/2019 - 10/24/2019 25 risky activities Filter



- Shared from SharePoint Online
- File(s) copied
- File(s) printed
- Email(s) sent externally
- Security tampering or harmful software
- Offensive language detected
- Others
- Compound

09/30/2019
HR Event: Resignation Date Set
 Resignation date set for: 10/11/2019

- Case details
- User details

About this case

Case name
IP Theft case

Case status
Active

Current risk level



Alerts confirmed
 Alert: Confidentiality obligation during departure

- Home
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
- Catalog
- More resources

Pseudonymize On **Open investigation** **Send e-mail notice** **Resolve case**

Case overview Alerts User activity **Content explorer** Social graph Case notes Contributors

>	Subject/Title	Date	Sender/Author	File class	Bcc
	Project Jupiter...			Document	
	Project Jupiter...			Document	
	Project Jupiter...			Document	
	Project Jupiter...			Document	
<input checked="" type="checkbox"/>	Project Jupiter...	10/17/2019, 8:58...	Talhah Mir	Document	
	Project Jupiter...			Document	
	item			Document	
	Project Jupiter...	10/17/2019, 8:58...	Talhah Mir	Document	
	Project Jupiter...	10/17/2019, 8:58...	Talhah Mir	Document	
	Project Jupiter...			Document	
	Project Jupiter...			Document	
	Project Jupiter...			Document	
	Project Jupiter...	10/17/2019, 8:58...	Talhah Mir	Document	
	Project Jupiter...	10/17/2019, 8:58...	Talhah Mir	Document	
	Project Jupiter...			Document	

1 item selected. 75 items total.

Escalate for data investigation

Escalate for employee investigation

File metadata

Source view

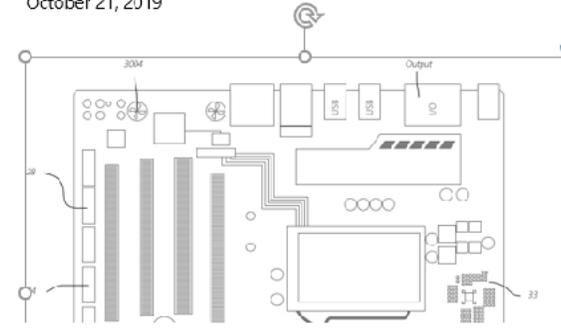
Word Accessibility Mode Print Find Immersive Reader

Contoso Electronics Top Secret

Project Jupiter

Updated Motherboard Design

Hardware Design Team
October 21, 2019



our new investments in hardware we need to redesign the AI500 motherboard to pull more throughput and reduce overheating. We have attached more fans to the

PAGE 1 OF 13 GIVE FEEDBACK TO MICROSOFT 89%

- Home
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - More resources

Case overview Alerts User activity **Content explorer** Social graph Case notes Contributors

Pseudonymize On Open investigation Send e-mail notice Resolve case

	Subject/Title	Date	Sender/Author
	Project Jupiter...		
<input checked="" type="checkbox"/>	Project Jupiter...	10/17/2019, 8:58...	Talhah Mir
	Project Jupiter...		
	item		
	Project Jupiter...	10/17/2019, 8:58...	Talhah Mir
	Project Jupiter...	10/17/2019, 8:58...	Talhah Mir
	Project Jupiter...		
	Project Jupiter...		
	Project Jupiter...	10/17/2019, 8:58...	Talhah Mir
	Project Jupiter...	10/17/2019, 8:58...	Talhah Mir
	Project Jupiter...		Document
	Project Jupiter...	10/17/2019, 8:58...	Document
	Project Jupiter...		Document

1 item selected. 75 items total.

Escalate for employee investigation

Create an employee investigation case for this user and notify the Employee Investigation Admins.

Name

Custodian
AnonyIS8-978

Source
Insider risk management

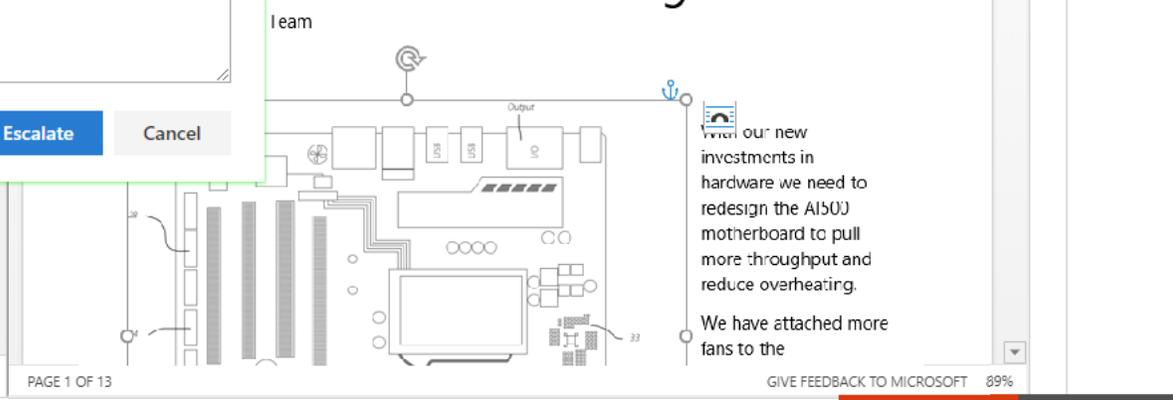
Note

Contoso Electronics Top Secret

Jupiter

ed Motherboard Design

Team



our new investments in hardware we need to redesign the AI500 motherboard to pull more throughput and reduce overheating. We have attached more fans to the

PAGE 1 OF 13

GIVE FEEDBACK TO MICROSOFT 89%



Communication Compliance

Communication compliance (preview)

Remove from navigation

Overview Alerts Policies **Notice templates**

+ Create policy ▾ Refresh ↻ Export policy updates

Monitor for offensive language	Reviewer
Monitor for sensitive info	adelev@scignite19.onmicro
Monitor for regulatory compliance	ccadmin@scignite19.onmicro
Custom policy	
Regulatory compliance - Brokers	ccadmin@scignite19.onmicro
Confidential project	ccadmin@scignite19.onmicro
Offensive language at Contoso	adelev@scignite19.onmicro
Code of conduct	ccadmin@scignite19.onmicro
Departing employees	adelev@scignite19.onmicro
Regulatory compliance Brokers FINRA	ccadmin@scignite19.onmicro
Emailing attachments to competitors	Reviewers@scignite19.onmicro

- CAPM Capital Asset Pricing Model
- CBO Collateralized Bond Obligation
- CD Certificate Of Deposit
- CDO Collateralized Debt Obligation
- CFD Contract For Differences
- CFTC Commodity Futures Trading Commission
- CHAPS Clearinghouse Automated Payment System
- CHIPS Clearinghouse Interbank Payment System
- CIF Cost, Insurance, Freight
- CLO Collateralized Loan Obligation
- CMO Collateralized Mortgage Obligation
- COD Cash On Delivery
- CP Commercial Paper
- CPI Consumer Price Index
- CPR Conditional Prepayment Rate
- CSA Credit Support Annex
- CTA Commodity Trading Advisor

9 items 🔍 Search

Escalated items	Resolved items
0	0
0	0
0	2
1	269
0	0
1	0
3	356
2	19
	2

Communication compliance > Create policy

- Name
- Users and reviewers
- Locations
- Conditions and percentage
- Finish

Choose supervised users and reviewers

Supervised users and groups *

Choose the users and group whose communications you want to supervise.

- All users
- Select users

Excluded users and groups

If you choose a group to supervise, you can exclude specific group members.

Reviewers *

Choose users or mail-enabled security groups to review the communications that are returned by this policy.



Communication compliance > Create policy

- ✓ Name
- ✓ Users and reviewers
- ✓ Locations
- Conditions and percentage
- Finish

Choose conditions and review percentage

Communication direction *

- Inbound.** Sent to users you choose to supervise from people not included in this policy.
- Outbound.** Sent to the users you choose to supervise to people not included in the policy.
- Internal.** Sent between the users or groups you identified in this policy.

Conditions

By default we will monitor all communications from the users and groups you specified. Add conditions to limit the results to communications matching specific criteria. [Learn more about these conditions](#)

+ Add condition ▾

Review percentage

If you want to reduce the amount of content to review, specify a percentage. We'll randomly select the amount of content from the total that matched any conditions you chose.

Slider control showing 100% review percentage.

Back Next

Cancel

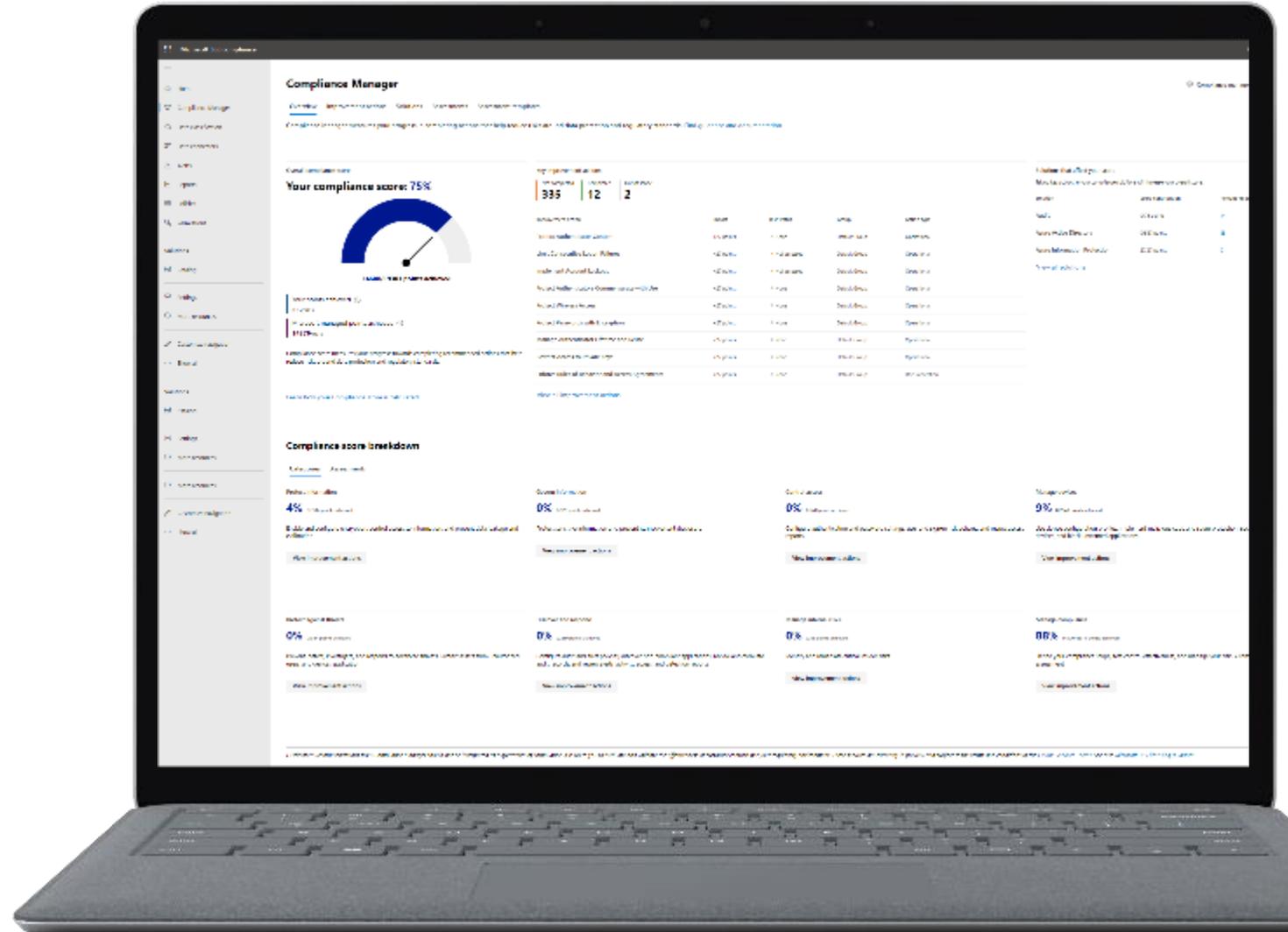


Compliance Management



Compliance Manager

Measure progress on your compliance journey, from taking inventory of your data protection risks to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

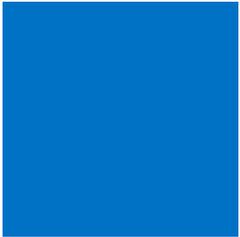




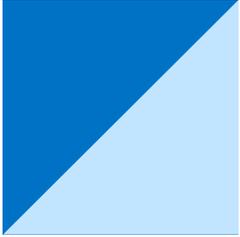
Demo

Compliance Manager

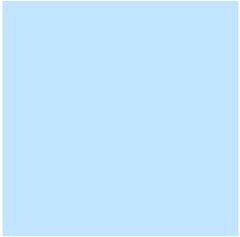
Shared Responsibility Model



Customer management of risk
Data Classification and data accountability



Shared management of risk
Identity & access management | End Point Devices



Provider management of risk
Physical | Networking

Cloud Customer Cloud Provider

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and accountability				
Client & end-point protection				
Identity & access management				
Application level controls				
Network controls				
Host Infrastructure				
Physical Security				

- Home
- Compliance score
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - More resources
 - Customize navigation
 - Show all

Microsoft Compliance Score

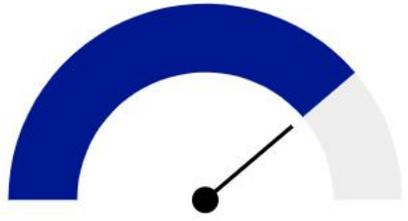
Overview Improvement actions Solutions Assessments

This service is currently in preview and is subject to the terms and conditions in the [Online Services Terms](#).

Filter

Overall compliance score

Your compliance score: 81%



18611/22936 points achieved

Customer-managed points achieved 1473/5798

Microsoft-managed points achieved 17138/17138

Compliance Score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

[Learn how Compliance Score is calculated](#)

Key improvement actions

Not completed: 345
 Completed: 61
 Not in scope: 0

Improvement action	Impact	Test status	Group
Disallow Simple Passwords on Mobile Devices	+27 points	Failed High Risk	Default Group
Implement Replay Resistant Authentication Mechanisms - Privile...	+27 points	Failed High Risk	Default Group
Enable Multi-factor Authentication for Admins	+27 points	Failed High Risk	Default Group
Register Users for Multi-Factor Authentication	+27 points	Failed High Risk	Default Group
Enable Sign-In Risk Policy	+27 points	Failed High Risk	Default Group
Authenticate to Cryptographic Module	+27 points	None	Default Group
Limit Consecutive Logon Failures	+27 points	None	Default Group
Automate Information Sharing Decisions	+27 points	None	Default Group
Automate Account Management	+27 points	None	Default Group

[View all improvement actions](#)

Solutions that affect your score

Taking key actions in your compliance solutions will increase your overall score.

Solution	Score contribution	Remain
Audit	30/88 points	14
Azure Active Directory	225/579 points	24
Azure Information Protection	0/27 points	1

[View all solutions](#)

Compliance score breakdown

Categories Assessments

- Home
 - Compliance Manager**
 - Data classification
 - Data connectors
 - Alerts
 - Reports
 - Policies
 - Permissions
 - Trials
-
- Solutions**
- Catalog
 - App governance
 - Audit
 - Content search
 - Communication compliance
 - Data loss prevention
 - eDiscovery

Compliance Manager

- Overview
- Improvement actions
- Solutions
- Assessments**
- Assessment templates
- Alerts
- Alert policies

Assessments help you implement data protection controls specified by compliance, security, privacy, and data protection standards, regulations, and laws. Assessments include actions that have been taken by Microsoft to protect your data, and they're completed when you take action to implement the controls included in the assessment. [Learn how to manage assessments](#)

Activated/Licensed templates
1/0

[View details](#)

4 items

Assessment	Status	Assessment progress	Your improvement act...	Microsoft actions
<input type="checkbox"/> Cyber Essentials 365	Pending update Incomplete	35%	19 of 260 completed	98 of 106 completed
<input type="checkbox"/> ISO/IEC 27001:2013	Pending update Not started	0%	0 of 583 completed	0 of 0 completed
<input type="checkbox"/> EU GDPR for Microsoft 365	Pending update Incomplete	26%	3 of 124 completed	19 of 19 completed
<input type="checkbox"/> Data Protection Baseline for Microsoft 365	Pending update Incomplete	60%	38 of 694 completed	681 of 706 completed



- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Trials

Solutions

- Catalog
- App governance
- Audit
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery

12 ISO/IEC 27001:2013

There is a pending update to this assessment [Review update](#)

Overview

- Details
- About

Progress Controls

Review improvement action status and view implementation

Improvement action status

None Not assessed

Accept all updates

Filter Reset Filter

Control family: Any

Improvement action

Add policies for apps with

- Control family**
- Cryptography
 - Physical and Environmental Security
 - Operations Security
 - Communications Security
 - System Acquisition, Development and Maintenance
 - Supplier Relationships
 - Information Security Incident Management
 - Information Security Aspects of Business Continuity Management
 - Compliance
 - Information Security Review
 - Information Security Policies
 - Organization of Information Security
 - Human Resource Security
 - Asset Management
 - Access Control
 - Improvement
 - Context of the Organization
 - Leadership
 - Planning
 - Support
 - Operation
 - Performance Evaluation

Refresh

Chat

- Search
- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Trials
- Solutions
- Catalog
- App governance
- Audit
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery

- Home
- Compliance score
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions

- Solutions
- Catalog
- More resources
- Customize navigation
- Show all

Compliance score breakdown

Categories Assessments

Data Protection Baseline

84% 13224/15602 points achieved

Product: Microsoft 365

Regulation: Data protection baseline

[View improvement actions](#)

GDPR / Office 365

64% 2850/4419 points achieved

Product: Office 365

Regulation: EU GDPR

[View improvement actions](#)

CCPA / Office 365

57% 277/480 points achieved

Product: Office 365

Regulation: CCPA

[View improvement actions](#)

ISO 27001 / Office 365

62% 4649/7404 points achieved

Product: Office 365

Regulation: ISO 27001

[View improvement actions](#)

NIST 800-53 / Office 365

83% 15037/18039 points achieved

Product: Office 365

Regulation: NIST 800-53

[View improvement actions](#)

FFIEC / Office 365

59% 3466/5837 points achieved

Product: Office 365

Regulation: FFIEC IS

[View improvement actions](#)

HIPAA / Office 365

72% 3176/4403 points achieved

Product: Office 365

Regulation: HIPAA/HITECH

[View improvement actions](#)

GDPR /Intune

48% 1182/2457 points achieved

Product: Intune

Regulation: EU GDPR

[View improvement actions](#)

FFIEC / Intune

55% 2534/4539 points achieved

Product: Intune

Regulation: FFIEC IS

[View improvement actions](#)

FedRAMP / Office 365

82% 15082/18210 points achieved

Product: Office 365

Regulation: FedRAMP Moderate

[View improvement actions](#)

NIST CSF / Office 365

74% 3168/4254 points achieved

Product: Office 365

Regulation: NIST CSF

[View improvement actions](#)

CSA CCM / Office 365

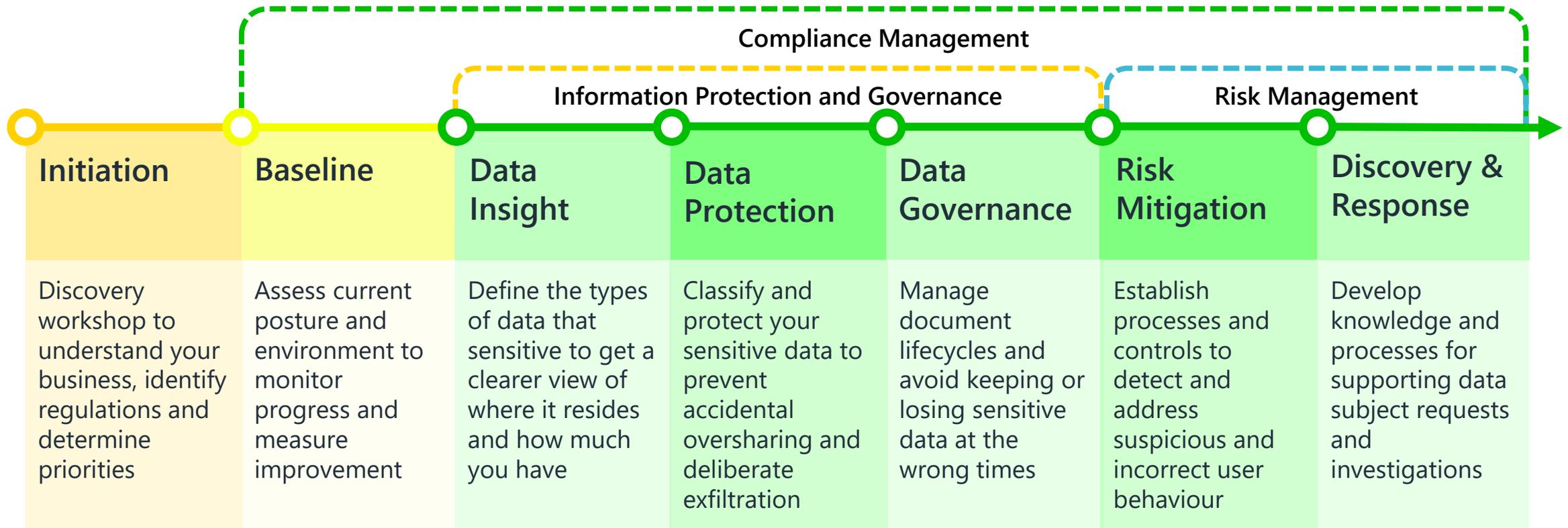
69% 5088/7308 points achieved

Product: Office 365

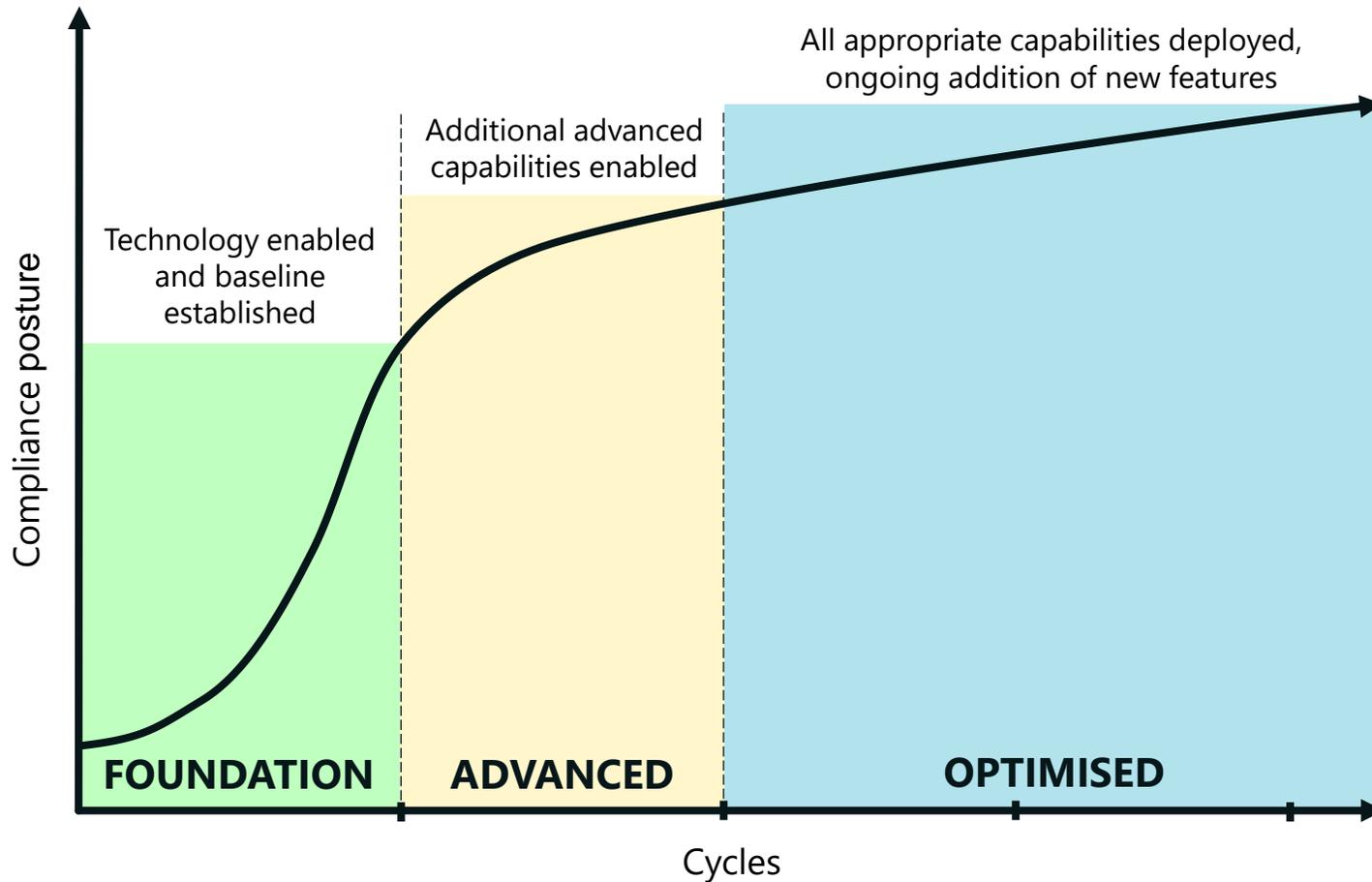
Regulation: CSA CCM

[View improvement actions](#)

Roadmap for Compliance

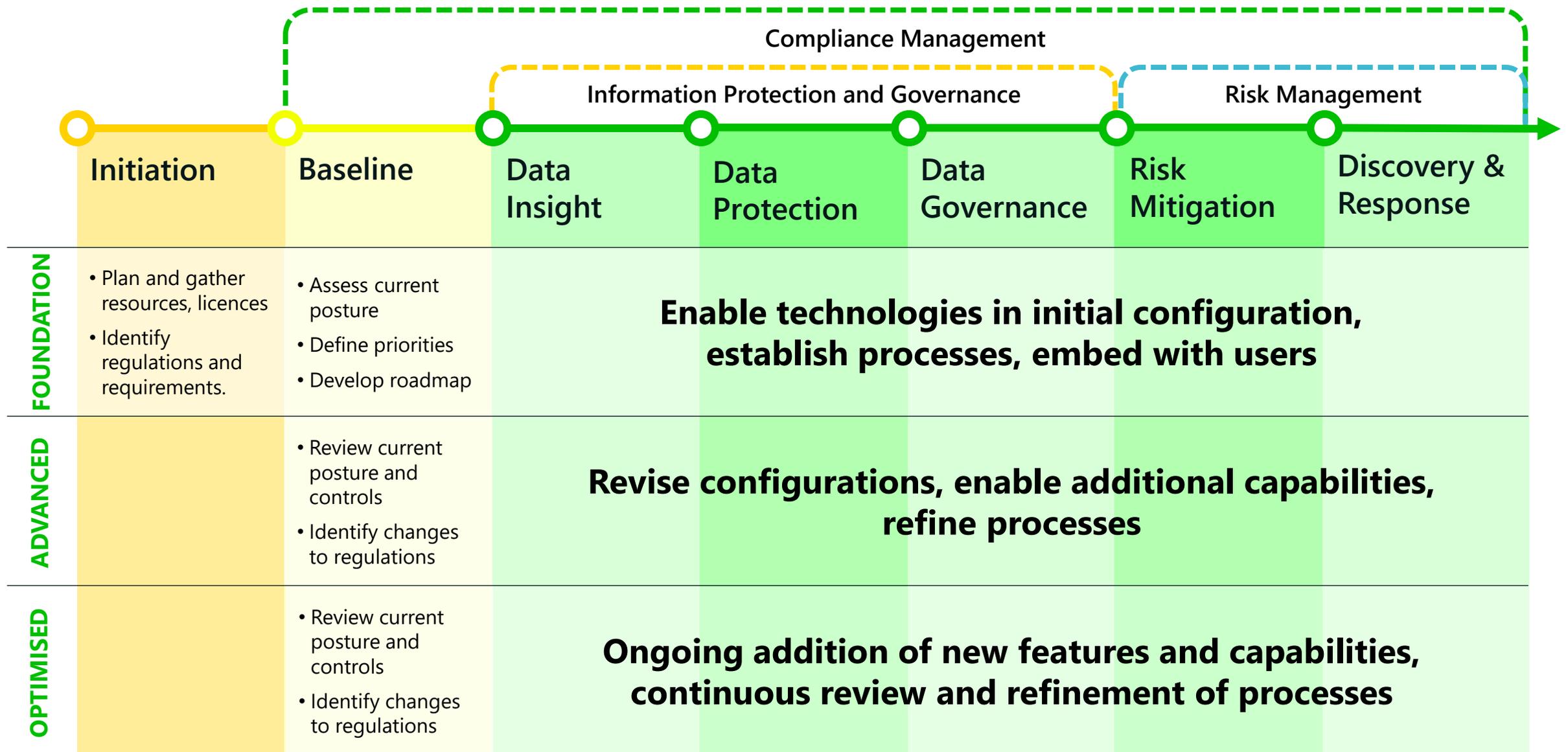


Compliance Success Pathway



Benefits of an iterative approach:

- Adapts to shifting business and regulatory priorities, and changes in the risk landscape
- Ensures new product and feature enhancements can be integrated as they are released
- Works within your budget to make clear progression along your compliance journey





Thank you

—————> Any questions?

Get in touch

To find out more about:

- Our Compliance Success Pathway approach to implementing your compliance strategy
- Further details of the individual compliance technologies

