Elkem

Plan, design, and pilot Microsoft Purview Data Security in 8 weeks

Gjert Tronstad, Cyber Security Director at Elkem

Atle Skjekkeland, CEO at Infotechtion, Microsoft MVP for Purview

About Elkem

- Elkem is a company that produces silicones, silicon, alloys for the foundry industry, carbon and microsilica, and other materials.
- Elkem was founded in 1904, has more than 7,000 employees and fields 30 production sites worldwide

Elkem

About Infotechtion

Infotechtion is a consulting and solutions provider specializing in data security and governance for Microsoft 365 and beyond.

Offices and staff in Norway, Netherlands, United Kingdom, United States, and India

Managed Professional Services	Add-on Solutions to Purview
Data Security and Governance strategy	Workspace Governance
POC as a Service and Production Pilots	Data Discovery and Security
Implementation advisory and program plans	AI Governance
Business change and training	Records Lifecycle

“I consider Infotechtion one of the leading experts in Microsoft information governance. Their staff work closely with our enterprise customers to maximize customer investment in Microsoft products especially Microsoft information protection and governance to enable increased levels of compliance for customer information in Microsoft 365.”
- Principal Engineering Manager, S+C Engineering, Microsoft.

Elkem

Know your data to secure your data

Data at risk of misuse if organization has no visibility into their data estate

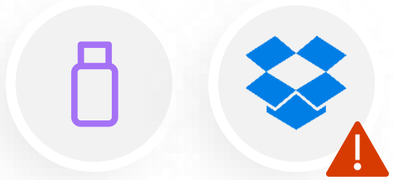
1

User falls prey to phishing attack, compromises user credentials

Data compromise by external threat

2

User copies file to a USB, then uploads to a personal Dropbox



Data theft by malicious insider

3

User inadvertently shares the file copy with a few colleagues

Data exposure by negligent insider

4

Artificial Intelligence use sensitive data to generate content

Data exposure by artificial intelligence

Leverage Microsoft Purview

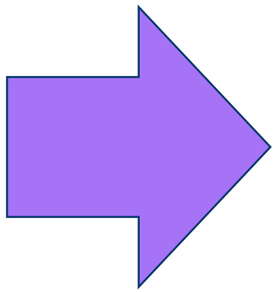
	Information Protection Identify and classify sensitive information	**eDiscovery** Respond to organisations' internal and external investigations	**Data Loss Prevention** Proactively protect known sensitive information	**Data Lifecycle Management / Records Management** Classify, Retain, Delete content	**Information Barriers** Restrict communication between groups and users to avoid conflicts of interest and safeguard internal information	**Communication Compliance** Minimize communication risks by detecting and acting on inappropriate messages	**Insider Risk Management** Correlate signals and activities to identify user intent
Pivot	Content	Content	Content	Content	User	User	User
Mitigation of Risk	**Rule enforcement:** Identify sensitive information type and protect and govern data **User Education:** Application of Sensitivity label	**Rule enforcement:** Create eDiscovery case to preserve data for investigation	**Rule enforcement**: Block action **User Education**: Show tips and show notification	**Rule enforcement:** Classify and Label content followed by applying retention policies **User Education:** Application of Record label	**Rule enforcement:** Detect and prevent unauthorized communication and collaboration among defined groups and users **User Education:** Show notification	**Rule enforcement**: Escalate to manager/legal for review **User Education**: Send notification	Collaboration across security, HR and legal
Examples	• Identification of sensitive documents • Protect sensitive information from being shared outside the organisation	• Collection, analyse, Review content to respond to legal matters	• Block printing of word documents with credit cards • Audit copying files with "Confidential" label to USB	• Inactive workspaces • Retaining/ Deleting content etc based on the compliance and legal requirements	• Stop some users from communication with each other via calls, chat, and email to avoid conflict of interest or safeguard internal information	• Check messages in your organization for unauthorized communications and conflicts of interest about confidential projects.	• Identify departing employees who are taking sensitive information with them • Identify vigilant insider threat of careful low-and-slow leaks over days

Elkem

Desired End state

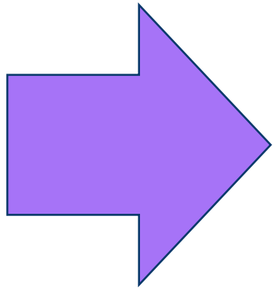
Infomation protection

Files/emails get the correct sensitivity label based on auto-classification (storage location, sensitive information types, trainable classifiers)



Data Loss prevention

Helps the users in performing the correct behaviours. This can be both blocking, guidance and supporting actions.



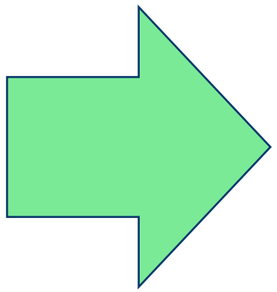
Insider risk management

Detects if users are circumventing the data loss prevention policies or are exhibiting unusual behaviours

Practical example

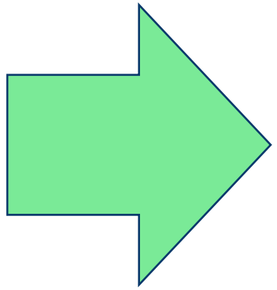
Infomation owner (Ellen)

Ellen creates a strategy document for an upcoming bid to acquire a different company. She ensures that the document is put in the project team and the document is classified as confidential based on the storage location



Infomation user (Bob)

Bob finds Ellen's document and want to share it with the accountant.
However, since the accountant is an external account, he gets blocked from sharing the document.



Infomation user

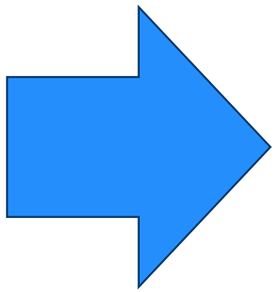
Bob decides to get around the block and downgrades the label before sharing once more. Since the sequence of actions Bob preformed is defined as extra risky by insider risk management, an alert is generated on Bob.

Technologies enabling the scenario

Infomation owner (Ellen)

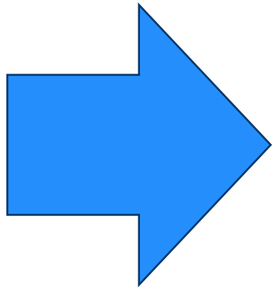
The company has labels without content marking and encryption

The workspace uses default label on the library as confidential ensuring classification based on location



Infomation user (Bob)

The company have a DLP policy in place blocking sharing files with the confidential labels with external accounts



Infomation user

Priority user group policy in place targeting every user that have access to insider information.

Plan, design, and pilot in 8 weeks

Before

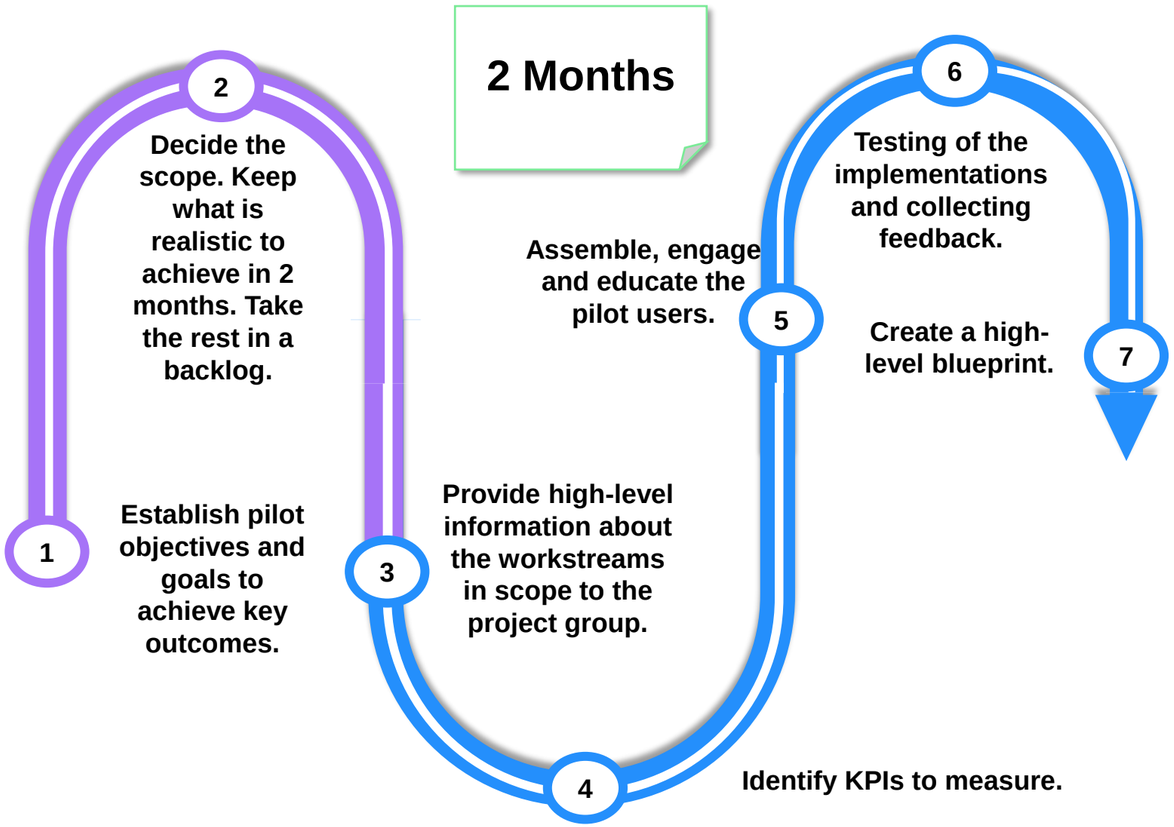
Elkem has Microsoft 365 with newly upgrade E5 license .

The goal was to design and pilot the following solutions:

- Microsoft Information Protection (MIP)
- Data Loss Prevention (DLP)
- Data Lifecycle Management (DLM)
- Insider Risk Management (IRM)

When the engagement ends, the client's technical team will be able to expand on what was done in the current scope.

Action



Pre-built templates to determine user stories and acceptance
Documented best practices to determine best approach for client
Recommendations by Infotechtion to ensure successful implementation

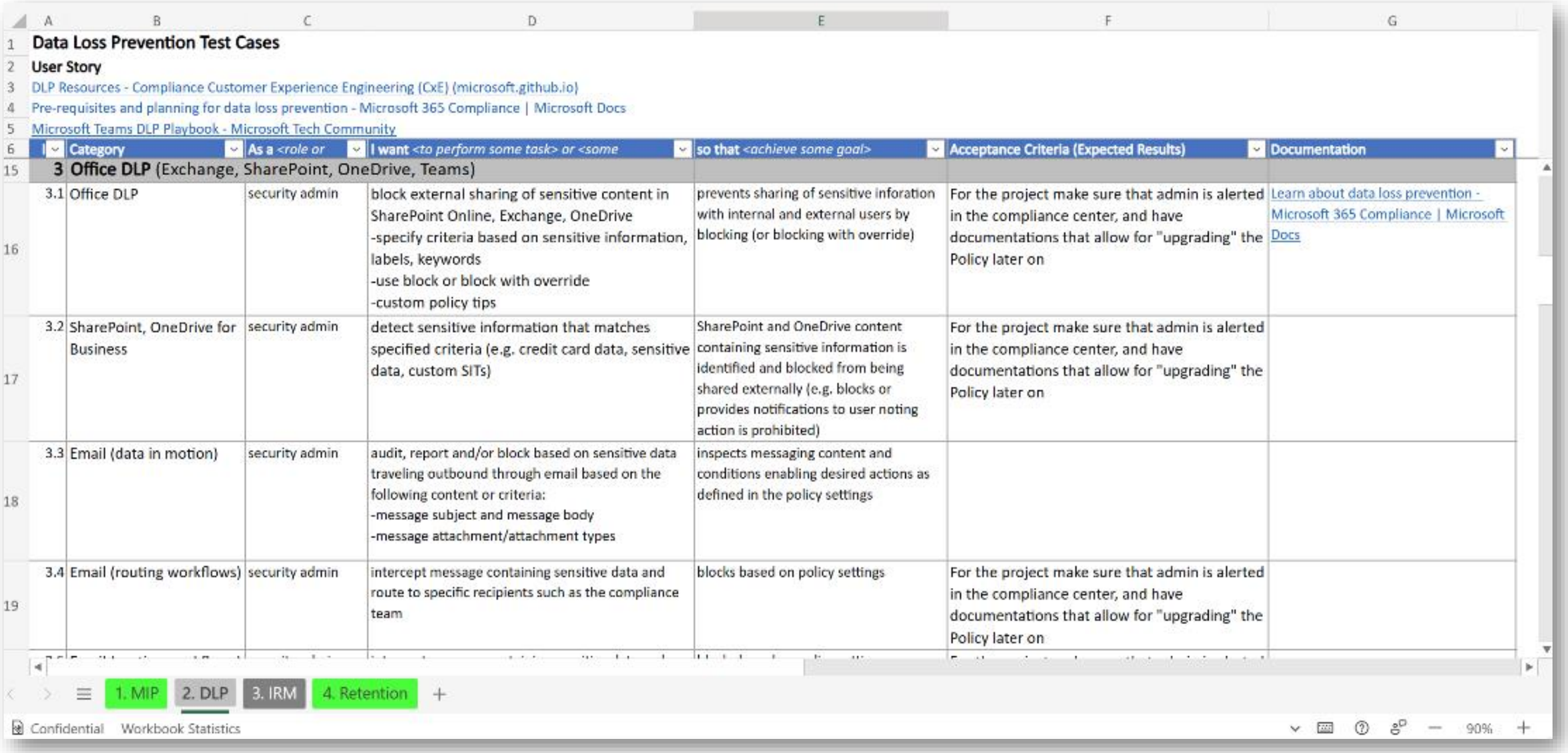
After

Outcomes:

- Blueprint documenting the implementation and recommendations for moving forward.
- Configuration sheets.
- Configuration of MIP, DLP, DLM and IRM in production tenant.
- Pilot with 40+ users testing MIP and DLM.
- Positive feedback.
- Education and awareness.
- DLP and IRM were tested and monitored by the project group
- Standard operating procedures
- Tools and knowledge to expand.

Elkem

Infotechtion templates to fast-track the implementation



Data Loss Prevention Test Cases

User Story

DLP Resources - Compliance Customer Experience Engineering (CxE) (microsoft.github.io)

Pre-requisites and planning for data loss prevention - Microsoft 365 Compliance | Microsoft Docs

Microsoft Teams DLP Playbook - Microsoft Tech Community

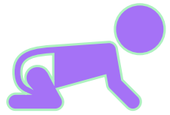
	Category	As a *<role or*	I want *<to perform some task> or <some*	so that *<achieve some goal>*	Acceptance Criteria (Expected Results)	Documentation
3	**Office DLP** (Exchange, SharePoint, OneDrive, Teams)					
3.1	Office DLP	security admin	block external sharing of sensitive content in SharePoint Online, Exchange, OneDrive -specify criteria based on sensitive information, labels, keywords -use block or block with override -custom policy tips	prevents sharing of sensitive inforation with internal and external users by blocking (or blocking with override)	For the project make sure that admin is alerted in the compliance center, and have documentations that allow for "upgrading" the Policy later on	Learn about data loss prevention - Microsoft 365 Compliance | Microsoft Docs
3.2	SharePoint, OneDrive for Business	security admin	detect sensitive information that matches specified criteria (e.g. credit card data, sensitive data, custom SITs)	SharePoint and OneDrive content containing sensitive information is identified and blocked from being shared externally (e.g. blocks or provides notifications to user noting action is prohibited)	For the project make sure that admin is alerted in the compliance center, and have documentations that allow for "upgrading" the Policy later on	
3.3	Email (data in motion)	security admin	audit, report and/or block based on sensitive data traveling outbound through email based on the following content or criteria: -message subject and message body -message attachment/attachment types	inspects messaging content and conditions enabling desired actions as defined in the policy settings		
3.4	Email (routing workflows)	security admin	intercept message containing sensitive data and route to specific recipients such as the compliance team	blocks based on policy settings	For the project make sure that admin is alerted in the compliance center, and have documentations that allow for "upgrading" the Policy later on	

1. MIP | 2. DLP | 3. IRM | 4. Retention

Confidential | Workbook Statistics | 90%

Elkem

The engagement and solution



CRAWL

Configure, publish labels and make them optional, supported by communications

WALK

Implement auto classification with more communications when people see them tied to their files.

RUN

Educate and operationalise the process for Alerts and resolution of new scenarios.

Establish and Strategy and Blueprint Design using Microsoft Data Security.

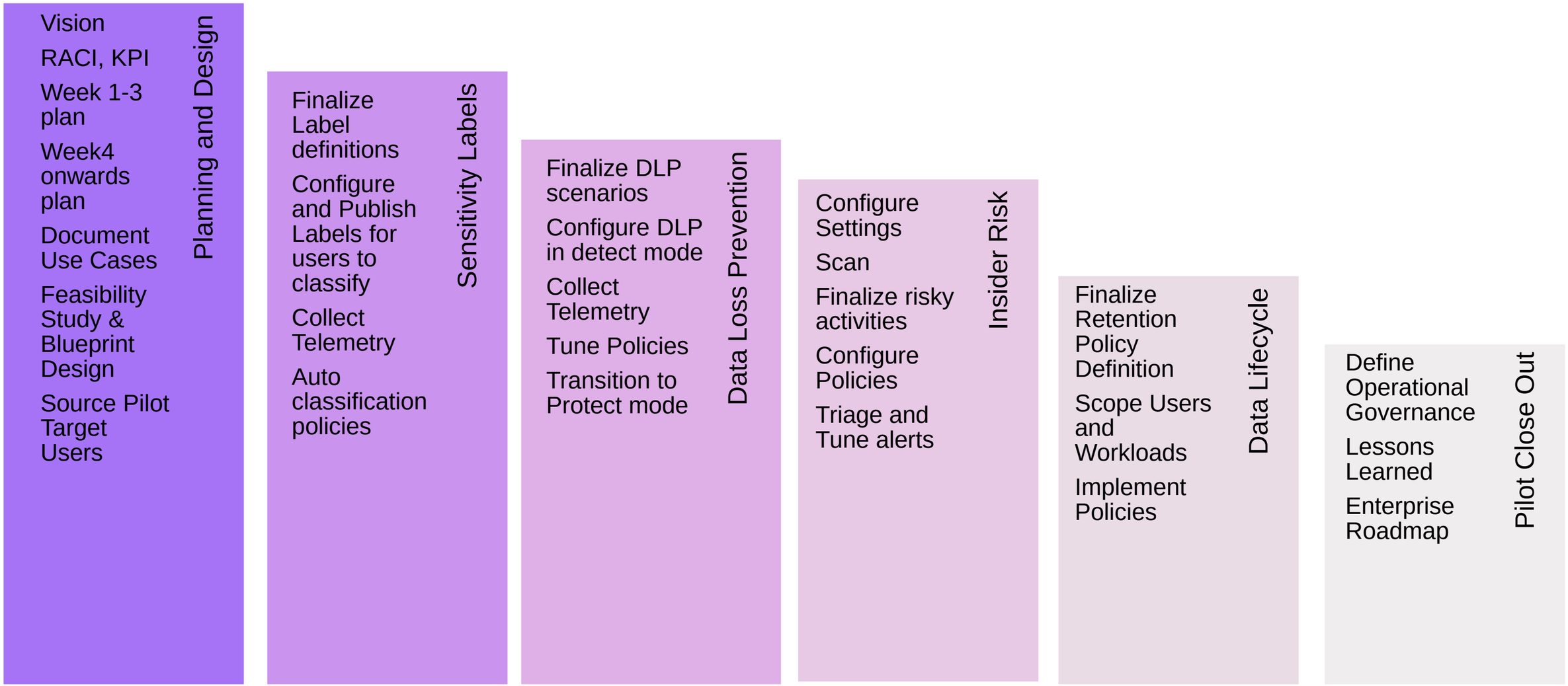
Implement in simulation mode and build the confidence in technology.

Activate education modes by first using the technology to inform users when working with sensitive data.

Enforce protection mode to prevent Data Loss , Over sharing , over retention and extreme data sabotage scenarios.

Elkem

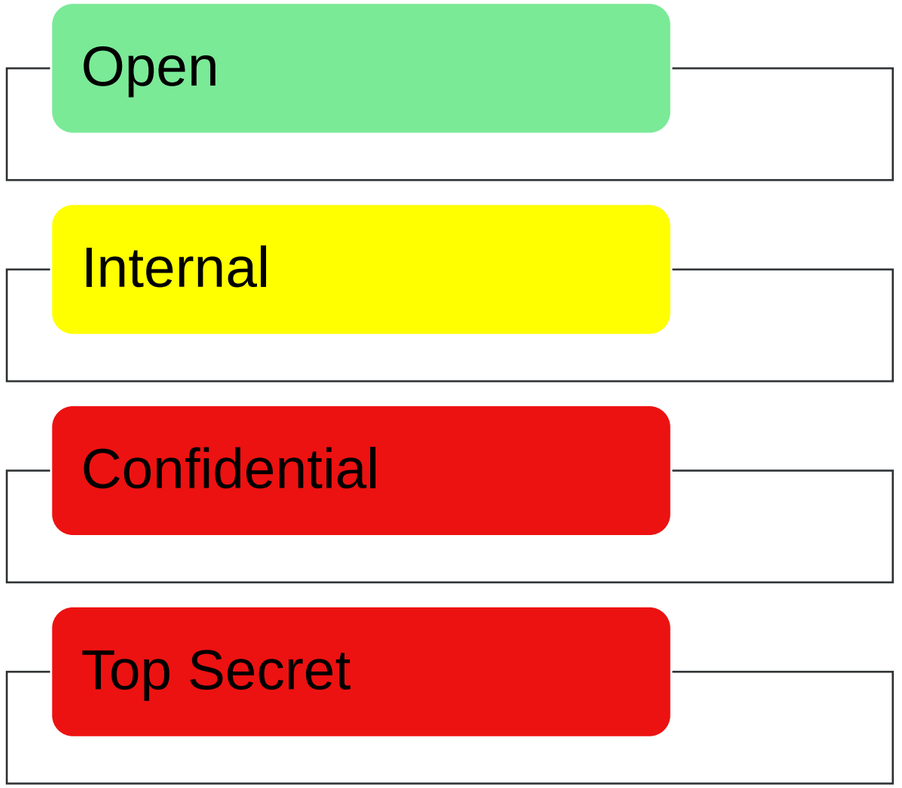
What was the approach over 8 weeks?



Elkem

Information Security Classification with Sensitivity Labels

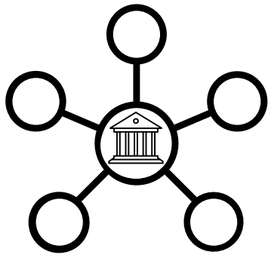
1. Establish only a few top-level classification levels
2. Only have sub-levels when this is justified
3. Consider linking access to security classification levels
4. Ensure the naming makes sense for users
5. Identify key words and phrases for each classification level
6. Ensure users only see relevant security classification levels
7. Decide if users should classify all information, or only exceptions
8. Establish increased protection levels per classification level
9. Find the correct balance between openness and control
10. Define use cases for external sharing of sensitive information



Sensitivity labels at Elkem

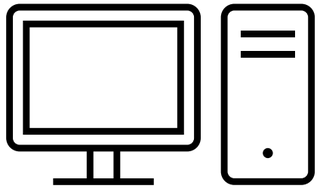
Open	**Internal**
Description: Use this label for content that is for public consumption. Marketing material, blogs etc. Color: Green	Description: Use this label for content that belong to the company but do not have any access limitations. Access limitation would be laws, policies and other rules that state the information need a specific classification. Color: Yellow
Confidential	**Top secret**
Description: Use this label for information that require stricter limitations due to law or regulations. Restricted files are not to be shared outside the organization without prior permission from the information owner. Color: Red WaterMark: Confidential Header: Watermark does not show up in mail so a header can be used to support the watermark Encryption: No	Description: This label is to be used for Elkems most sensitive information. The information should not be shared with anyone outside the organization unless strictly necessary. Color: Red WaterMark: Top secret Header: Watermark does not show up in mail so a header can be used to support the watermark Encryption: No

Data Loss Prevention (DLP)



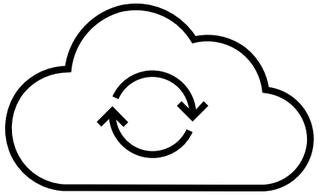
Network

Monitors all incoming and outgoing data on the organizations network and prevents unauthorized data transfer



Endpoint

Monitors endpoint devices such as desktops or laptops and prevents data leakage

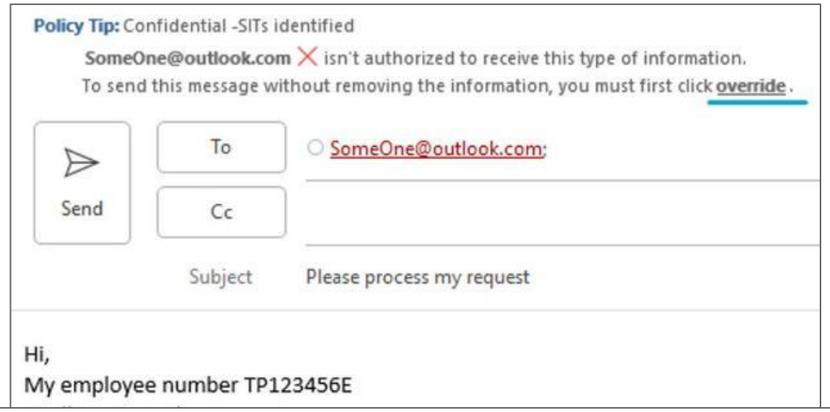


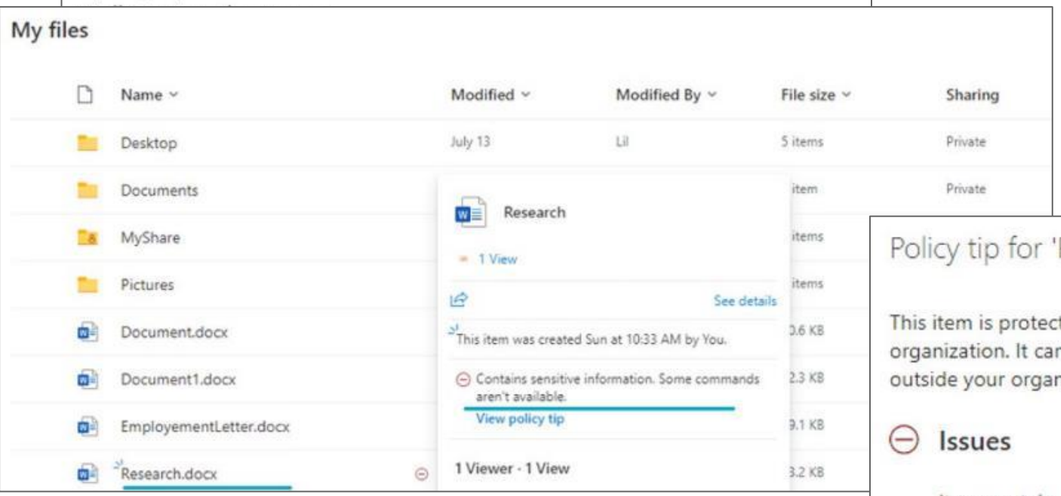
Cloud

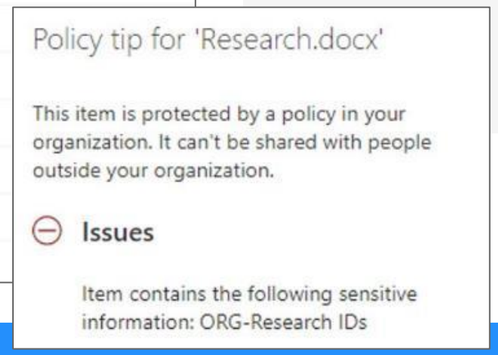
Ensures that data stored in the cloud are not leaked or mishandled, and prevents unauthorized access or sharing of cloud data

Data Loss Prevention with Policy Tips

DLP Exchange policy with user overrides:

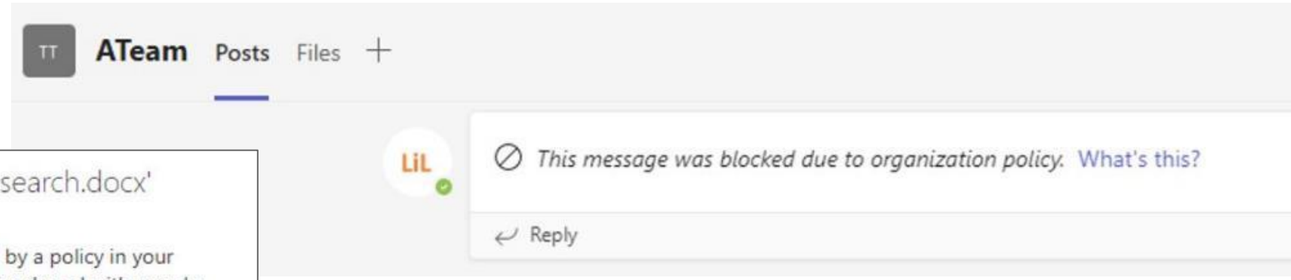






DLP Teams policy with block – for sender:

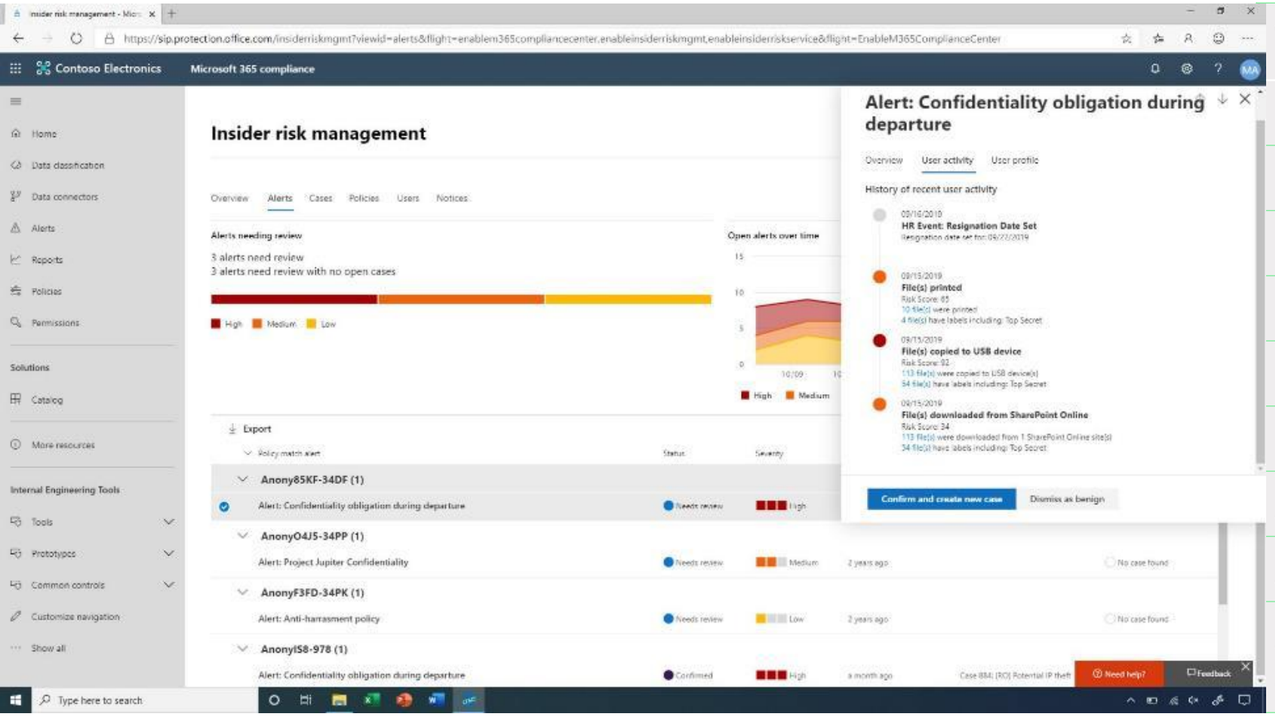
DLP Teams policy with block – for receiver:



Prevent data loss based by establishing rules to only allow data transfer / sharing through an allowed list of sequences and transfer channels.

Elkem

Insider Risk Management

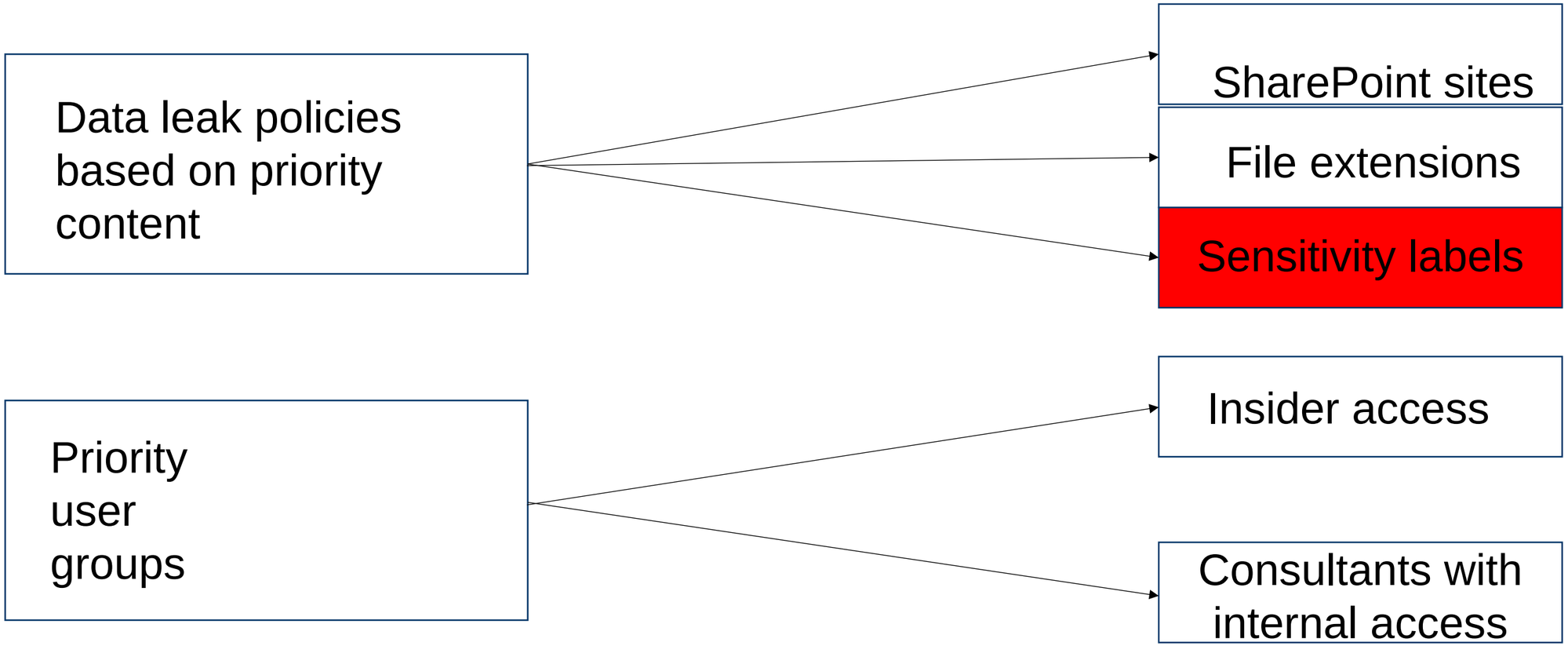


Which User Behaviours to Monitor and Manage?
Sent to non-corporate external email
Stored with open permissions
Shared externally with unvetted listed identities
Uploaded to personal cloud storage
Saved to removable storage
Printed
Accessed in non-business hours (at 2AM)
Accessed from not logical geolocation (Company don’t operate)
Accessed/stored in functionally inaccurate locations (financial data stored on an HR site)

Protect company value when employees leave and / or users identified as high priority working with most sensitive data / processes.

Elkem

Insider risk management (crawl)



Data Lifecycle Management recommendations

- Apply shorter retention to 1:1 or group chats in Microsoft Teams.
- Apply Longer retention to Posts and conversations in Microsoft Team channels.
- Manage retention for Teams meeting recordings.

Conversations

- A Non-Record Deletion policy for emails.
- An Information architecture for managing emails identified as long-term records.
- A process for archiving records to support employee leaver process.

Communication

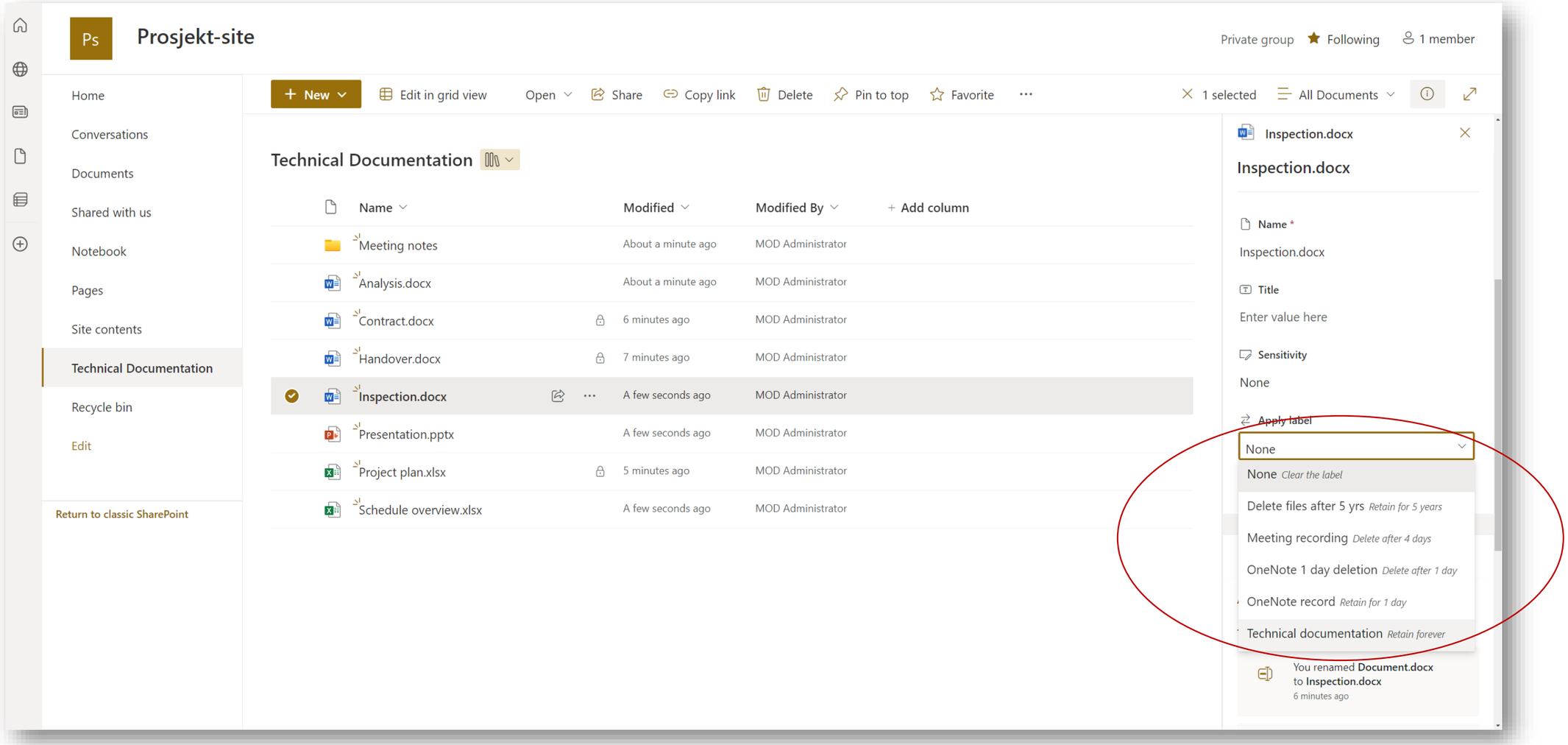
- A non-record deletion policy for files in OneDrive, Teams, SharePoint.
- Auto-classification of all information matching the corporate retention classification scheme.
- A disposition review process for audit of long-term records.

Files

Elkem

Files in shared workspaces

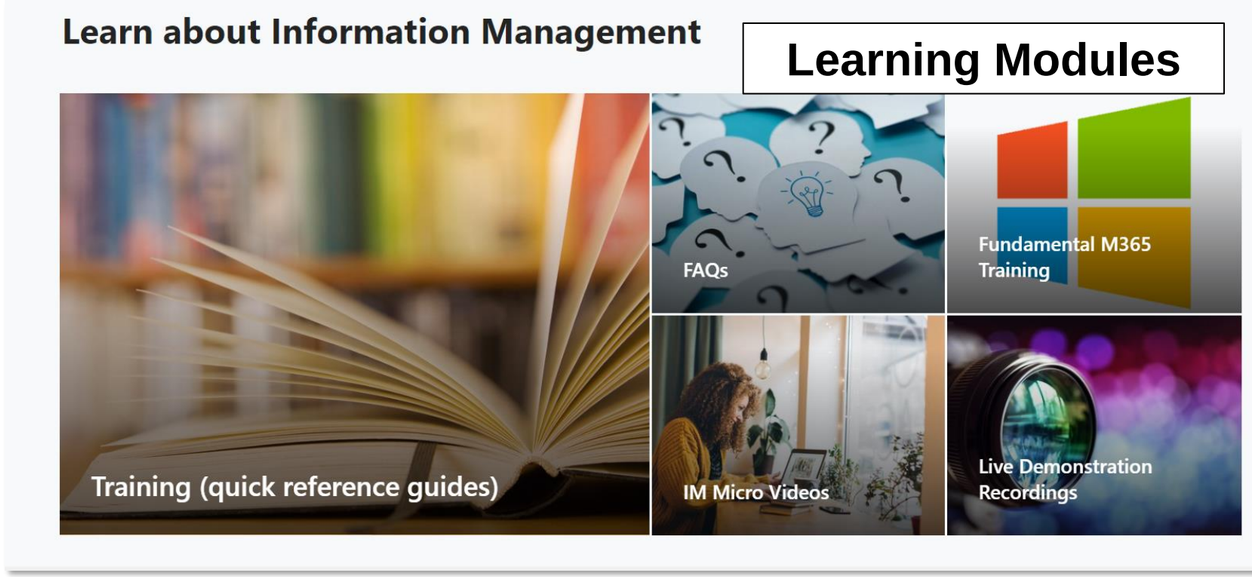
Keep what we need of files in shared workspaces with Record labels, then delete what we don’t need.



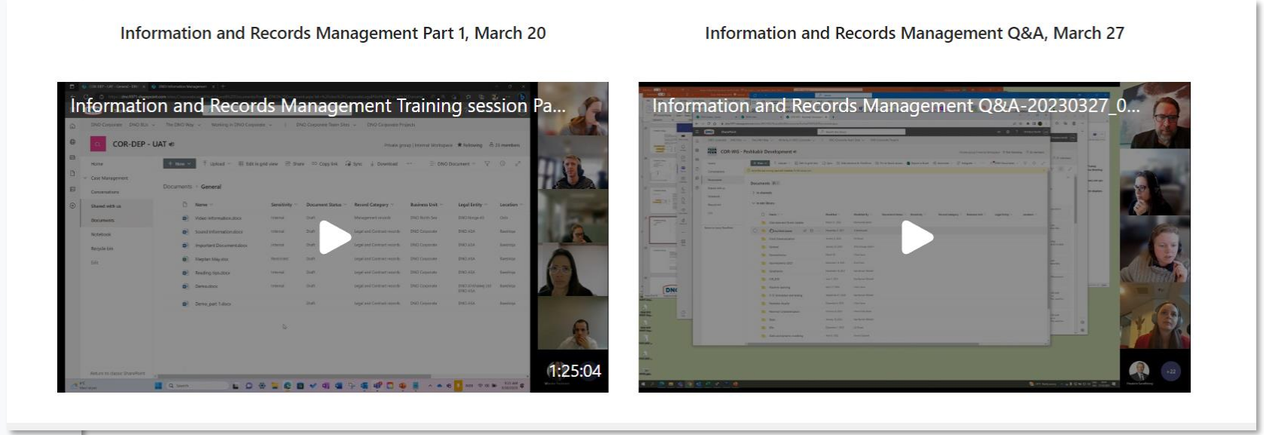
Elkem

Communication and education

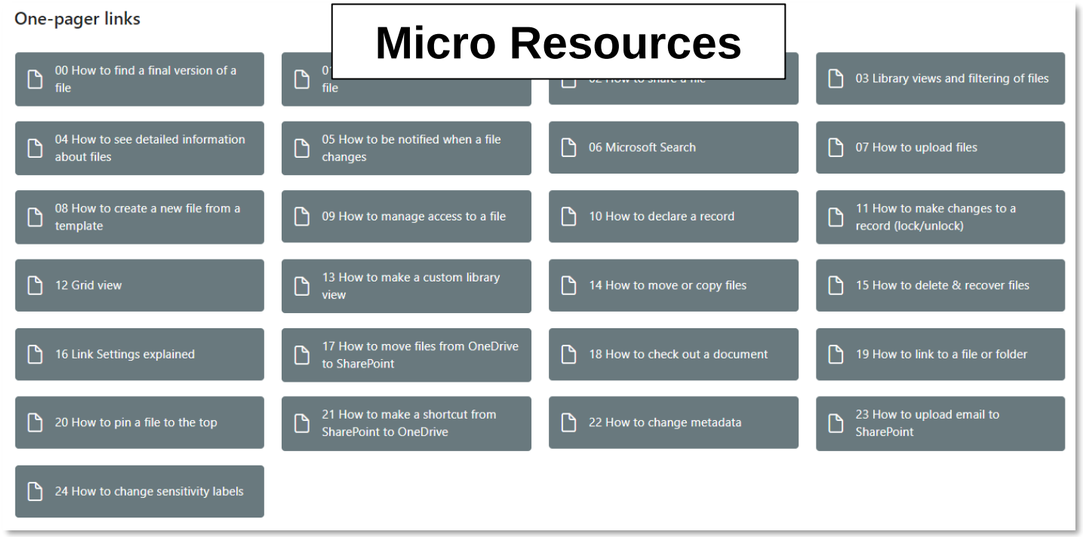
Learning Modules



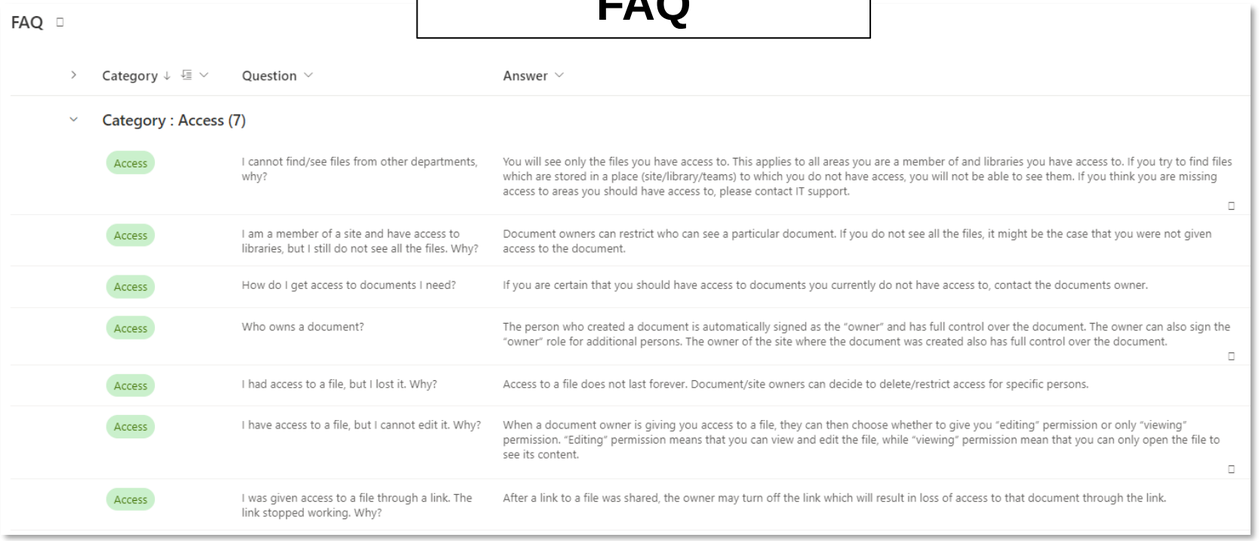
Live sessions



Micro Resources



FAQ



Elkem

Planned monitoring and metrics

Workspace

- Inactive Teams
- Teams without Owner
- Public Teams
- Teams without Hub
- Empty Teams
- Deleted Teams
- Teams with less than 2 Members
- Teams without IG & Security baseline configurations

Content

- Count of Files shared internally
- Count of files shared externally
- Content on HOLD after deletion
- Content without a lifecycle
- Sensitive and Shared externally with anonymous access
- Users in exception for Anonymous external sharing
- Links shared externally more than 3 months ago.

Compliance

- Teams at 90% storage quota
- Total Data leak alerts
- Microsoft365 compliance score
- Approved exceptions to IG baseline
- Workspaces at risk of deletion due to no action by Team owners
- Total files with higher sensitivity than Workspaces.

Adoption

- Learning resource hub page hits
- Training adoption on roles, responsibilities related to IG.
- Team Owners default category due to missing role attestation deadlines.
- Total active users actively classifying files.

Implementation Objectives (8 weeks)

Activate E5 compliance for defined Pilot users

Based on identified risks and use cases, validate the technical design that needs to be covered leveraging E5 Compliance features.
Technical guidance to configure and activate the E5 compliance features at the platform level to enable Microsoft Information Protection, Data Loss Prevention, and Insider Risk Management.
Provide an overview of the advanced features and benefits of E5 compliance, and the relevance of features to meet the use cases.
Technical guidance in deployment of Auto labelling for sensitivity labelling with E5 compliance features to autodetect sensitive information and automatically tag files.
Document standard operating procedures for managing alerts and insights generated from configurations. Provide feedback and reporting on lessons learned, KPIs etc. that can be used to inform an enterprise rollout.

Primary Objective: Implement a solution to manage risks related to sensitive data loss by configuring automation of data classification, data loss prevention and data lifecycle management

Elkem

Questions

Email:

- Gjert.Tronstad@elkem.com
- Atle.S@infotechtion.com

Web:

- www.elkem.com
- www.infotechtion.com