Microsoft Purview Information Protection & Data Loss Prevention Kick-Start Guide V3

Content

msftcompliance.com | LinkedIn | Twitter | All Things M365 Compliance

1 Introduction

1.1 Background

Microsoft Purview Information Protection and Data Loss Prevention Solutions are designed to help organisations protect their sensitive data across various platforms and environments. They offer features such as sensitivity labelling, data discovery, data analysis, data reporting, data collection, and data exploration. These features enable organisations to classify, monitor, and control their data according to their policies and regulations.

1.2 Purpose

As a Microsoft Purview Compliance qualified architect, I have worked with diverse organisations across various industries, especially those operating under strict regulatory frameworks. I have found great satisfaction in helping them implement and optimise Microsoft Purview Solutions for their data protection needs. Although, I have faced some challenges in finding the precise information I need on Microsoft Docs and other resources. While these resources are comprehensive and valuable, they are also voluminous and scattered, making it difficult to locate specific information efficiently.

To address this issue and ensure seamless conversations with customers and colleagues, I have created this comprehensive guide. It serves as a consolidated resource, providing topical information on solutions, roles, features, and relevant links for further exploration. With this guide at your fingertips, you can access vital information without interruptions or the need to leave ongoing conversations or meetings.

1.3 Scope

This guide covers the following Microsoft Purview Information Protection and Data Loss Prevention Solutions:

- Sensitivity Labelling – Auto Labelling and Manual Labelling
- Labelling Client Versions
- Data Loss Prevention
- Endpoint Data Loss Prevention
- Data Discovery; Cloud & On-Premises
- Data Analysis
- Data Reporting
- Data Collection & Explorers

To bolster your organisation's defence-in-depth strategy, this guide goes beyond Information Protection and Data Loss Prevention to encompass additional Compliance and Security solutions. These solutions are designed to integrate with your existing measures, providing enhanced protection and comprehensive coverage for your sensitive data.

Exploring these supplementary solutions can further fortify your organisation's security posture and ensure compliance with industry regulations. These solutions offer a range of features and functionalities that address various aspects of data protection, risk management, and threat detection.

From Insider Threat/Risk solutions that help identify and mitigate internal security risks to Defender for Cloud Apps and Sentinel that offer advanced threat protection and real-time monitoring, to creating data segmentation with Discovery & Respond Solutions, this guide presents a rounded approach to safeguarding your organisation's data.

Specifically, it includes insights into:

- Insider Threat & Insider Risk
- Cloud App Security for Information Protection*[1]
- Compliance Boundaries*[2]
- Customer Lockbox*[3]
- Information Barriers*[4]
- Defender for Cloud Apps*
- Microsoft Sentinel*[5]

1.4 Structure

This guide is divided into sections and sub-sections that follow a logical order and progression. Each section provides an introduction, an explanation of the solution or feature, and links to relevant resources for further exploration. Each section also includes a summary that highlights the main points and implications of the solution or feature.

1.5 License Requirements

To help you understand the license requirements for each solution or feature, I have indicated the license type in brackets after the solution or feature name. The markers used are as follows: (E3) indicates an E3 License requirement, and (E5) indicates an E5 License requirement. While Microsoft offers Bolt-On Licenses, I have chosen not to include them as license markers within this document to simplify the information. However, you can refer to the Licensing Matrix link below for detailed entitlement information should you need to verify license requirements.

This guide aims to facilitate your understanding of Microsoft Purview Information Protection and Data Loss Prevention Solutions, offering valuable insights in a single, easily accessible location. It equips you with the necessary resources to:

- Understand the solutions in depth.
- Get started with implementing the solutions effectively.
- Develop comprehensive designs tailored to your specific needs.
- Create or extend labelling taxonomies for Sensitivity Labelling.
- Prepare for and implement configurations that provide optimal protection for your organisation-sensitive data.

These readily available resources have proven immensely valuable to me, and I trust that this guide will offer you the same advantages.

[1] Defender for Cloud Apps aka Cloud App Security is a Microsoft Defender Product
[2] Compliance Boundaries is an eDiscovery Solution (Discover & Respond)
[3] Customer Lockbox is an Insider Risk Product
[4] Information Barriers is an Insider Risk Product
[5] Sentinel is a Security Product

2 Microsoft's Four Pillars of Compliance

Microsoft breaks down the Purview Compliance Solutions into 4 stages:

2.1 Know Your Data

This is the first and most important step as this provides the organisation with a chance to understand the data landscape and identify sensitive or important data across Cloud and On-Premises. This enables the migration of data into the required workloads or identifies data that requires labelling before migrating to Cloud for regulatory purposes.

2.2 Protect Your Data

The Protect Your Data segment provides the organisation with the ability to protect data with encryption via Information Protection Sensitivity Labelling either with Microsoft Keys, Bring Your Own Keys or Double Key Encryption for File, Email, and supported items within SharePoint Libraries. As well as enabling granular access controls to SharePoint, Teams, and Microsoft Groups via Container Level Labelling. Additionally, Microsoft offers Office Message Encryption; Basic & Advanced and extending Sensitivity Labelling to Microsoft Defender for Cloud Apps.

2.3 Prevent Data Loss

The Prevent Data Loss segment allows the organisation to configure DLP Policies for data:

- in motion
- in use
- at rest

These policies help prevent intentional or accidental oversharing of sensitive information. The segment also enables extending DLP for Microsoft Defender for Cloud Apps to control connected third-party apps for data inspection.

2.4 Govern Your Data (Not covered in this guide)

The Govern Your Data segment provides the organisation with the means to:

- retain data based on policies and labels,
- create a defensible disposal strategy with data disposition reviews,
- the ability to retain data in M365 for the organisation to govern.
- support regulatory compliance requirements by marking items as immutable or retaining versions.

3 Data Classification

Data Classification is a crucial capability that empowers organisations to effectively identify, tag, and review M365, On-Premises and Third-Party data. It offers automated methods to apply labels to data, enabling detailed content review and analysis of user activities. This feature is particularly valuable for organisations that heavily rely on Keyword Dictionaries and Lexicon Libraries, as it enables data classification and exploration.

In the context of auto-labelling, the configuration heavily depends on data classifications to ensure accurate labelling of data. By leveraging predefined classifications, organisations can ensure that data is appropriately labelled, enhancing data governance and security measures. The automated nature of data classification streamlines the labelling process, reducing manual effort and improving overall efficiency in managing and protecting sensitive information.

To achieve this Microsoft offers the following solutions:

- Trainable Classifiers (TCs)
  - Automated Data Matching via Classifiers
- Sensitive Information Types (SITs)
  - Automated Data Matching via Keywords and Lexicons
- Exact Data Match (EDM)
  - Automated Data Matching via Exact Data Value Matching
- Content Explorer (CE)
  - View Matched Data Content
- Activity Explorer (AE)
  - View Users Tenant Activity

By leveraging data classification solutions across Microsoft 365 services, organisations can enforce consistent data protection policies, enhance compliance efforts, and effectively manage and secure sensitive information.

3.1 Sensitive Information Types

Sensitive Information Types are predefined patterns or templates designed to identify specific types of sensitive information within an organisation's data. They play a crucial role in data protection and are utilised in features such as Data Loss Prevention (DLP) and Sensitivity Labels. Microsoft offers a wide range of over 300 preconfigured Sensitive Information Types that cover various sensitive data categories.

These prebuilt types include common data patterns like:

- Financial information
- International personal information
- Computer information types

Additionally, Microsoft provides the flexibility to create custom Sensitive Information Types tailored to meet the specific needs and requirements of your organisation. This allows you to align the detection and protection of sensitive information with your internal policies and compliance obligations, ensuring a comprehensive and effective information protection strategy.

Sensitive Information Types can be used in various locations within Microsoft 365, including:

- Exchange Online
- SharePoint Online
- OneDrive for Business
- Microsoft Teams
- Microsoft 365 Apps (Word, Excel, PowerPoint, etc.)

With both preconfigured and custom options at your disposal, you can proactively safeguard sensitive data and maintain regulatory compliance, bolstering your organisation's information protection strength.

3.2 Trainable Classifiers

Trainable classifiers are machine learning models trained to identify and classify specific types of content or data within an organisation's environment. These classifiers are part of the Sensitivity Labelling and Data Loss Prevention (DLP) solution and can be trained to recognise sensitive information, such as Personally Identifiable Information (PII) or financial data, based on patterns and characteristics.

Trainable Classifiers are machine learning models that can:

- Identify and classify specific types of content or data within an organisation’s environment based on patterns and characteristics.

- Recognise confidential data, such as Personally Identifiable Information (PII) or financial data, in various contexts, including emails, documents, and other types of files.

- Learn from examples provided by administrators or end-users, allowing them to adapt and improve their accuracy over time.

3.3 Exact Data Match

Exact Data Match (EDM) is a feature that enables organisations to pinpoint and protect specific occurrences of sensitive data within their environment: it permits your organisation to define custom data patterns or sequences that are unique to your organisation and use them to detect and classify sensitive information. You can configure these patterns and scan various data sources, such as emails, documents, and databases, to identify matches.

Exact Data Match (EDM) based classification offers several advantages:

- Dynamic and Easy Refresh: EDM-based classification allows for easy updates and refreshes of sensitive information types, ensuring that the classification remains accurate and up to date.

- Reduced False-Positives: By using exact data matching, EDM-based classification minimises the occurrence of false-positive results, providing more reliable identification of sensitive data instances.

- Compatibility with Structured Data: EDM is specifically designed to handle structured sensitive data, making it an ideal solution for organisations dealing with data in specific formats, such as databases or spreadsheets.

- Enhanced Data Security: With EDM, sensitive information is handled securely, as the data is not shared with anyone, including Microsoft. This ensures that organisations maintain complete control and confidentiality over their sensitive data.

- Integration with Microsoft Cloud Services: EDM-based classification can be seamlessly utilised with various Microsoft cloud services, allowing organisations to extend the benefits of accurate classification and protection across their digital ecosystem.

Exact Data Match can be used with the following services:[6]

Service	Locations
Microsoft Purview Data Loss Prevention	- SharePoint Online
	- OneDrive for Business
	- Teams Chat
	- Exchange Online
	- Devices
Microsoft Defender for Cloud Apps	- SharePoint Online
	- OneDrive for Business
Auto-labelling (Service Side)	SharePoint Online
	OneDrive for Business
	Exchange Online
Auto-labelling (Client Side)	Word
	Excel
	PowerPoint
	Exchange desktop clients
Customer Managed Key	SharePoint Online
	OneDrive for Business
	Teams Chat
	Exchange Online
	Word
	Excel
	PowerPoint
	Exchange desktop clients
	Devices
eDiscovery	SharePoint Online
	OneDrive for Business
	Teams Chat
	Exchange Online
	Word
	Excel
	PowerPoint

[6] Table from Microsoft. Learn Exact Data Match

	Exchange desktop clients
Insider Risk Management	SharePoint Online
	OneDrive for Business
	Teams Chat
	Exchange Online
	Word
	Excel
	PowerPoint
	Exchange desktop clients

3.4 Viewing Sensitive Data - Content Explorer (E5 feature)

Content Explorer is a powerful tool that helps you protect your organisation's sensitive information and data activity. It lets you access and review all the files and emails that contain sensitive information across various services, such as

- SharePoint Online
- OneDrive for Business
- Exchange Online
- Teams

It also shows you how Sensitive Information and Sensitivity Labelling are being used in your environment, so you can:

- Find and label files and emails that contain sensitive information types, such as credit card numbers or personal identification numbers, with the appropriate sensitivity level, such as Confidential or Highly Confidential.

- See who has access to your sensitive files and emails, and what actions they have taken on them, such as opening, editing, or sharing.

- Generate reports and dashboards to monitor the usage and effectiveness of Sensitive Information and Sensitivity Labelling across your organisation and identify areas for improvement.

With Content Explorer, you can gain valuable insights into your organisation's sensitive information and data activity and take action to ensure compliance and security.

Note:
Content Explorer permissions should be granted only to trusted users, as it allows them to view the full content of the items they review. This can help them protect your organisation's sensitive information and data activity, but it also requires them to respect the privacy and confidentiality of the data owners.

3.5 Viewing User Activity – Activity Explorer (E5 feature)

Activity Explorer is a feature in Microsoft 365 that allows your organisation to track and analyse user activities across various Microsoft 365 apps and services, such as:

- SharePoint Online
- OneDrive for Business

- Exchange Online
- Teams

Admins can use Activity Explorer to see files users have:

- Accessed
- Shared
- Collaborated on

As well as other actions such as:

- File Creation
- Deletion
- Modification
- Download
- Upload

Activity Explorer can help you monitor users' behaviour and identify any potential security and compliance risks in your organisation, such as data leakage, unauthorised access, policy violations, etc. For example, you can use Activity Explorer to see who has accessed or shared a sensitive file outside the organisation, who has deleted or modified a critical file without permission, who has downloaded or uploaded many files in a short period of time, etc. By using Activity Explorer, you can gain valuable insights into your users' productivity and data protection in Microsoft 365.

3.5.1 Recent Changes

Microsoft has now provided the ability to view some Data Loss Prevention and File Activities to Activity Explorer which are the following:

- Endpoint DLP activities.
- Files containing sensitive info types.
- Egress activities.
- DLP policies that detected activities.
- DLP policy rules that detected activities.

Additionally, administrators can view DLP Overrides and Items that match a DLP Rule. This is a great way to see DLP activities within a single pane of glass.

These can be identified with the below activities:

Information	Activity
Users Override	DLP Rule Undo
Items that match a DLP Rule	DLP Rule Matched

3.5.2 Contributing Links:

- Get Started with Content Explorer:
  - Get started with content explorer - Microsoft 365 Compliance | Microsoft Docs
- Get Started with Activity Explorer:
  - Get started with activity explorer - Microsoft 365 Compliance | Microsoft Docs
- Labelling Activity Reference:

  - Labeling actions reported in Activity Explorer - Microsoft 365 Compliance | Microsoft Docs
- Increase Classifier Accuracy (Preview):
  - Increase Classifier Accuracy - Microsoft Purview (compliance) | Microsoft Learn
- DLP Activity Explorer and Reports:
  - Learn about data loss prevention - Microsoft Purview (compliance) | Microsoft Learn

4 Microsoft information Protection | Sensitivity Labelling (E3 & E5)

Sensitivity Labels are a feature in Microsoft 365 that allows your organisation to classify and protect its data based on its level of sensitivity. You can use Sensitivity Labels to apply classifications and protections to files, emails, and meetings, as well as Microsoft Groups and Sites. For example, you can use Sensitivity Labels to mark a document as Confidential or Highly Confidential, encrypt an email with a specific recipient list, add a watermark to a presentation, or restrict access to a SharePoint site.

You can apply Sensitivity Labels in the following ways:

- Manual Labelling: The user applies the label onto the item manually, choosing from a list of available labels. The label can also detect the sensitive information included in the item and suggest the appropriate label for the user.

- Auto-Labelling | Client-Side: The labelling client in use, such as Office apps or Outlook, detects a Sensitive Information Type in the item and automatically applies the label that is configured with that type. For example, if the client detects a Credit Card Number or a Social Security Number in a document or an email, it can apply a label that marks it as Highly Confidential and encrypts it.

- Auto-Labelling | Service-Side: The Service-Side Labelling engine scans files and emails stored in Microsoft 365 services, such as SharePoint Online or Exchange Online, and detects the Sensitive Information Types in them. It then applies the label that is configured with those types. For example, if the engine detects a Bank Account Number or a Passport Number in a file or an email, it can apply a label that marks it as Confidential and adds a watermark.

4.1.1 Labelling Options

Labels are a feature in Microsoft 365 that allows your organisation to classify and protect its data based on its level of sensitivity. You can use Labels to apply classifications and protections to items, groups and sites, meetings, and schematised data assets. Labels can be configured with numerous options depending on the label's use case.

Here are some of the options available to you:

4.1.1.1 Label Names and Descriptions (Items & Groups and Sites):[7]

You can define unique names and descriptions for your sensitivity labels to accurately represent the purpose and level of sensitivity they convey. When providing descriptions, I highly recommend you include enough information to ensure the users are aware of the severity of the label and the data it maps to. For example, you can use names and descriptions like:

[7] It is important to note that Names cannot be changed once published.

- Public: This label is for data that is intended for public disclosure or has no confidentiality requirements.
- General: This label is for data that is intended for internal use only or has low confidentiality requirements.
- Confidential: This label is for data that is intended for authorised users only or has moderate confidentiality requirements.
- Highly Confidential: This label is for data that is intended for restricted users only or has high confidentiality requirements.
- Label Colours (Items): Labels can be configured with colours to represent the severity of the classification. I always advise using the Traffic Light system to order Labels, Green being the least sensitive, Amber being the moderate sensitivity and Red being the most sensitive.

For example, you can use colours like:

Colours	Reason
Green	For Public label
Yellow	For General label
Orange	For Confidential label
Red	For Highly Confidential label

4.1.1.2 Label Scopes (Items, Groups and Sites & Databases)

Enable the destination required for Labels. The destination determines where the label can be applied and how it affects data protection. For example, you can enable scopes like:

- Items include a) Files, b) Emails, and c) Meetings. These are individual items that can be labelled by users or automatically by policies. The label can apply encryption, watermarking, header/footer, or other protections to the items.
- Groups & Sites include a) SharePoint Sites, b) Teams Channels, and c) M365 Groups. These are containers that can be labelled by owners or administrators. The label can apply encryption, permissions, or other protections to the containers and their contents.
- Meetings include Meetings in Outlook and Teams. These are events that can be labelled by organisers or attendees. The label can apply encryption, access control, recording policy, or other protections to the meetings and their contents.
- Schematized Data Assets include SQL, Azure SQL, Azure Cosmos DB’s and more. These are databases that can be labelled by owners or administrators. The label can apply encryption, masking, auditing, or other protections to the databases and their records.

4.2 Shared Experiences on Labelling

4.2.1 The Importance of Sensitivity Labelling

From my extensive experience in the field of Microsoft Purview Compliance, I can confidently say that Sensitivity Labelling is a highly desired solution among organisations. It quickly becomes apparent that organisations are eager to implement robust information protection measures by establishing a comprehensive Classification Taxonomy, or as Microsoft refers to it, a Sensitivity Labelling Taxonomy.

The importance of Sensitivity Labelling cannot be overstated, as it enables organisations to effectively categorise and protect their most sensitive data. By assigning specific labels to different types of information, organisations gain granular control over data access, sharing, and security. This enables them to enforce policies and controls that align with their unique compliance requirements and data protection goals.

Some of the benefits of Sensitivity Labelling are:

- It helps organisations to identify and classify their data assets based on their level of sensitivity, such as Public, General, Confidential, or Highly Confidential.
- It allows organisations to apply encryption, watermarking, header/footer, retention, or other protections to their data assets based on their labels.
- It enables organisations to restrict access, sharing, or use of their data assets based on their labels and the recipient's identity or location.
- It assists organisations to comply with industry regulations and standards, such as GDPR, HIPAA, PCI-DSS, or ISO 27001.

4.2.2 The Process of Classification Taxonomy

Implementing a well-defined Classification Taxonomy is a crucial step in ensuring the successful deployment of Sensitivity Labelling. By carefully designing and structuring the Labelling Taxonomy, organisations can accurately classify their data assets and establish a solid foundation for effective information protection. This process requires a thorough consideration of data types, organisation requirements, and regulatory obligations to ensure that the Labelling Taxonomy reflects the organisation's specific needs.

Some of the steps of Classification Taxonomy are:

- Identify the types of data that your organisation handles and stores, such as personal data, financial data, health data, intellectual property, etc.
- Define the levels of sensitivity for each type of data based on its confidentiality, integrity, and availability requirements.
- Create labels for each level of sensitivity and assign them names, descriptions, colours, and icons that accurately represent their purpose and severity.
- Configure policies and controls for each label based on the desired protection actions and conditions for your data assets.

- Test and validate your labels and policies before applying them to your data assets.

4.2.3 The Good Practices for Labelling Deployment

When it comes to Labelling Deployment, Microsoft has Three-stages on how to roll out Labels into your organisation. This comes in the form of Crawl, Walk, Run. Many organisations want to use Client-Side Auto-Labelling because it is easier for the users. This way, they can avoid depending on individuals to select the right Label for the data and the recipient. They can also reduce the risk of users not choosing a Label at all because they do not know how sensitive the data is or how to label it. However, this is not recommended, Crawl is the first step into a Labelling Deployment, and that means manual labelling.

It is very important to dedicate time and offer training before rolling out Labelling Deployment. This will help you increase user awareness, adoption, and compliance with your classification and protection policies. You should train and educate your users on how to identify the data and the Sensitivity Label that maps to it. For example, you can use demos, videos, topical questions, or feedback to show your users how to label their data assets manually or automatically. You can also explain the impact and benefits of labels on their data access, sharing, and security.

Taking the time to thoroughly plan and deploy your classification taxonomy, and gradually rolling it out to a select group of users within departments, is crucial for a smooth and successful implementation. Rushing the process can lead to chaos and undesirable consequences for your organisation and its users. I've witnessed first-hand the aftermath of a rushed deployment, where over one hundred thousand items were mistakenly encrypted, resulting in weeks of effort to undo the encryption and regain access to the blocked documents. It was a challenging and stressful experience for everyone involved, and it's certainly a situation your organisation would want to avoid at all costs.

Some of the best practices for Labelling Deployment are:

- Start with manual labelling (Crawl): Train your users on how to identify and label their data assets manually. This will help them understand the importance of classification and protection and the impact of labels on their data assets.

- Move to client-side auto-labelling (Walk):[8] Enable your users to use the labelling clients, such as Office apps or Outlook, to automatically detect and label their data assets based on the sensitive information types or content they contain. This will help them save time and effort and ensure consistent and accurate labelling across their data assets.

- Advance to service-side auto-labelling (Run):[9] Enable the service-side labelling engine to scan and label your data assets stored in Microsoft 365 services, such as SharePoint Online or Exchange Online, based on the sensitive information types or content they contain. This will help you cover all your data assets and enforce your policies and controls across your organisation.

[8] This ensures your organisation has defined an accurate Sensitive Information Types program of work.
[9] This ensures your organisation has defined an accurate Sensitive Information Types program of work.

4.2.4 The Importance of Classification Taxonomy

I would like to share an important aspect with you. I often have conversations with organisations that have yet to compose a Classification Taxonomy. As a result, they will try to assemble the classification taxonomy as they build out the sensitivity labelling design and configurations. As you can imagine, this takes a huge amount of time and effort to work through, due to building out the core configurations without that important baseline labelling taxonomy to work with. Add to that the complexities of navigating around the permissions, reasons for allowing internal and external sharing, who should or should not see the labels and how many labels are needed. I have witnessed this process several times now and it never works out as expected! I encourage you to take the time to assemble a Labelling Taxonomy before building out a Sensitivity Labelling Taxonomy.

4.2.5 The Steps of Classification Taxonomy

When creating a Sensitivity Labelling Taxonomy, consider the following main points:

Data Classification: Start by identifying and classifying the different types of data within your organisation. Understand the sensitivity levels and regulatory requirements associated with each type of data. For example, you can classify your data into types such as:

- Personal data: Data that relates to an identifiable individual, such as name, email address, phone number, home address, national insurance, or social security numbers etc.

- Financial data: Data that relates to the financial transactions or records of your organisation or its customers, such as invoices, bank statements, credit card numbers, trade deals, mergers, and acquisitions, etc.

- Health data: Data that relates to the health or medical conditions of your organisation or its customers, such as medical records, prescriptions, test results, etc.

- Intellectual property: Data that relates to the creative or innovative output of your organisation or its employees, such as patents, trademarks, designs, etc.

4.2.6 Label Hierarchy

A clear hierarchy for sensitivity labels is important because it helps you to organise and manage your labels based on their level of sensitivity. A hierarchy consists of parent and child labels, where the parent label represents a broad category of sensitivity, and the child label represents a specific subcategory of sensitivity. For example, you can have a parent label called “Confidential” and two child labels called “Confidential Internal” and “Confidential Trusted Recipients”.

The parent label defines the general level of sensitivity for the data, while the child labels define the specific permissions and protections for the data based on who can access it. For example, you can use the following hierarchy as an example:

- Public (Non-Organisation Sensitive): This label is for data that is intended for public disclosure or has no confidentiality requirements.

- Confidential: This parent label is for data that is intended for authorised users only or has moderate confidentiality requirements.

  - Confidential Internal: This child label is for data that is intended for internal use only within your organisation.
  - Confidential Trusted Recipients: This child label is for data that is intended for external use only with trusted recipients who have a contractual or legal obligation to protect the data and need a business justification to access it.

- Highly Confidential: This parent label is for data that is intended for restricted users only or has high confidentiality requirements.
  - Highly Confidential Internal: This child label is for data that is intended for internal use only within a specific group or department within your organisation.

  - Highly Confidential Trusted Recipients: This child label is for data that is intended for external use only with trusted recipients who have a contractual or legal obligation to protect the data and need a business justification to access it.

Label Names and Descriptions: Use descriptive and intuitive names for your sensitivity labels. Ensure that the label names align with your organisation's terminology and are easily understandable by users. Do not expose organisation names or sensitive data in the terms. For example, you can use names and descriptions like:

- Public (Non-Organisation Sensitive): "This label is for data that is intended for public disclosure or has no confidentiality requirements. Apply this label to data that can be freely shared with anyone without any risk or impact to your organisation".

- Confidential Internal: "This label is for data that is intended for internal use only within your organisation. Apply this label to data that contains confidential information that should not be shared outside your organisation without authorisation".

- Highly Confidential Trusted Recipients: "This label is for data that is intended for external use only with trusted recipients who have a contractual or legal obligation to protect the data or may need a business justification to access it. Apply this label to data that contains highly confidential information that should only be shared with specific external parties under strict conditions".

Label Permissions and Protection: Determine the permissions and protection settings associated with each sensitivity label. Specify who can access, edit, and share data labelled with different sensitivity levels. It is not uncommon to have multiple-label policies if the need for them is met. For example, you can use permissions and protection settings like:

- Public (Non-Organisation Sensitive): No permissions or protection settings are required for this label, as the data can be freely accessed, edited, and shared by anyone.

- Confidential Internal: This label can apply encryption, watermarking, header/footer, or retention to the data. The permissions can restrict access to internal users only and prevent external sharing or forwarding.

- Highly Confidential Trusted Recipients: This label can apply encryption, watermarking, header/footer, or retention to the data. The permissions can restrict access to specific external recipients only and require a business justification and an overriding reason for sharing or forwarding.

Label Application: Define the scenarios and conditions under which each sensitivity label should be applied. Consider factors such as content type, location, and user roles when determining when to apply specific labels. For example, you can use scenarios and conditions like:

- Public (Non-Organisation Sensitive): This label should be applied to data that is publicly available or has no confidentiality requirements, such as marketing materials, press releases, newsletters, etc.

- Confidential Internal: This label should be applied to data that is intended for internal use only or has moderate confidentiality requirements, such as employee records, financial reports, project plans, etc.

- Highly Confidential Trusted Recipients: This label should be applied to data that is intended for external use only with trusted recipients who have a contractual or legal obligation to protect the data and need a business justification to access it, such as contracts, agreements, proposals, etc.

4.2.7 User Education and Awareness

Develop training materials and communication strategies to educate users about the sensitivity labelling taxonomy. Promote awareness of the importance of correctly applying sensitivity labels to ensure data protection and compliance. For example, you can use training materials and communication strategies like:

- Demos, videos, quizzes, or feedback to show your users how to label their data assets manually or automatically using Office apps or Outlook.

- Newsletters, posters, webinars, or workshops to inform your users about the impact and benefits of labels on their data access, sharing, and security.

- Surveys, polls, interviews, or focus groups collect feedback from your users about their experience and satisfaction with the labelling taxonomy.

4.2.8 Review and Iteration

Regularly review and refine your sensitivity labelling taxonomy based on feedback, evolving organisation needs, and changes in regulatory requirements. Continuously improve and adapt the taxonomy to maintain its effectiveness. For example, you can review and iterate your labelling taxonomy by:

- Monitoring and analysing the usage and performance of your labels and policies using reports and dashboards.

- Identifying and resolving any issues or gaps in your labelling taxonomy using audits and alerts.

- Updating and enhancing your labels and policies based on new data types, organisation requirements, or regulatory obligations.

4.2.9 Legacy Labelling Taxonomy

Clients who find themselves in the opposite position face the predicament of having a well-defined classification taxonomy with sophisticated mappings of data types to labels. Despite this advantage, they encounter obstacles when attempting to migrate this taxonomy into the M365 environment.

These challenges primarily stem from issues related to naming conventions or the presence of legacy labelling structures.

Some of the challenges are:

- Naming conventions that are inconsistent or incompatible with the M365 Sensitivity Labels model. For example, using acronyms, abbreviations, or organisation names that are unclear or confusing for users or administrators.

- Legacy labelling structures that are outdated or redundant with the M365 Sensitivity Labels model. For example, using labels that are established on retention or disposition rather than sensitivity, or using labels that are no longer relevant or applicable to the organisation.

4.2.9.1 The Consequences of Incorrect Deployment of Sensitivity Labels

The deployment of sensitivity labels may be adversely affected. The process may be delayed as the organisation grapples with the complexities of converting its existing taxonomy into the appropriate Sensitivity Labelling framework. This delay can impede the organisation's ability to effectively protect and manage its sensitive data. Furthermore, in some cases, incorrect deployment of sensitivity labels may occur due to confusion or misinterpretation during the migration process. This can lead to subsequent challenges and difficulties that arise after the labels have been deployed. Resolving these issues can be time-consuming and require significant effort, adding further complexity to the overall information protection strategy. I recently had the opportunity to assist two organisations in redesigning their labelling taxonomy, and I must admit that the process can be quite demanding.

Some of the consequences are:

- Delayed deployment of sensitivity labels prevents the organisation from applying classification and protection to their data assets promptly.
- Incorrect deployment of sensitivity labels that causes errors or inconsistencies in data access, sharing, and security, resulting in a redesign and redeployment.

- Subsequent challenges and difficulties require troubleshooting and remediation after the labels have been deployed. This can be very disruptive.

4.2.10 Recommendations for a Transition to Sensitivity Labels

It is crucial for organisations to carefully evaluate their existing classification taxonomy and ensure a seamless transition to the Sensitivity Labels model within M365. By addressing naming conventions and aligning with good practices, organisations can avoid potential difficulties and ensure a smooth deployment of sensitivity labels that effectively protect their sensitive data assets.

Some of the recommendations are:

- Review and revise naming conventions to ensure they are descriptive, intuitive, and consistent with the M365 Sensitivity Labels model. For example, use names that reflect the level of sensitivity and purpose of the label, such as Public, General, Confidential, or Highly Confidential.

- Review and remove legacy labelling structures that are outdated or redundant with the M365 Sensitivity Labels model. For example, use labels that are based on sensitivity rather than retention or disposition, and use labels that are relevant and applicable to the organisation.

- Test and validate sensitivity labels before deploying them to ensure they work as expected and meet the organisation's requirements. For example, use a pilot group of users or locations to test the labels and policies before applying them to all users or locations.

4.3 Contributing Links:

- Protect your sensitive data with Microsoft Purview
  - Microsoft Purview Information Protection - Microsoft Purview (compliance) | Microsoft Learn
- Deploy an information protection solution with Microsoft Purview
  - Deploy an information protection solution with Microsoft Purview - Microsoft Purview (compliance) | Microsoft Learn
- Microsoft Purview Information Protection Deployment Acceleration Guide: Crawl, Walk Run:
  - Microsoft Information Protection and Data Loss Prevention - Compliance Customer Experience Engineering (CxE)
- Designing a Classification Framework for M365 Labelling:
  - Create a well-designed data classification framework - Microsoft Service Assurance | Microsoft Docs
- Classification aka Labelling Taxonomy:
  - Data classification & sensitivity label taxonomy - Microsoft Service Assurance | Microsoft Docs
- Learn about Labels:
  - Learn about sensitivity labels - Microsoft 365 Compliance | Microsoft Docs
- Get Started with Labels:
  - Get started with sensitivity labels - Microsoft 365 Compliance | Microsoft Docs
- Compare AIP Add-In with Built-In Labelling in M365 Apps:
  - CompareAIP2MIP - Microsoft Purview Customer Experience Engineering (CxE)
- MIP: Notes from the field:
  - https://techcommunity.microsoft.com/t5/security-compliance-identity/mip-notes-from-the-field/ba-p/1501297
- Scope labels to just Files or Emails:
  - https://learn.microsoft.com/en-gb/microsoft-365/compliance/sensitivity-labels-office-apps?view=o365-worldwide#scope-labels-to-just-files-or-emails
- Use sensitivity labels to protect calendar items, Teams meetings, and chats:
  - Use sensitivity labels to protect calendar items, Teams meetings, and chat - Microsoft Purview (compliance) | Microsoft Learn
- External Sharing Scenarios:

  - Secure external collaboration using sensitivity labels - Microsoft Tech Community
- Restrict Access to Content via Labels:
  - Restrict access to content using sensitivity labels to apply encryption - Microsoft 365 Compliance | Microsoft Docs
- Considerations for Encrypted Content:
  - https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide#considerations-for-encrypted-content
- A small troubleshooting guide for auto-applying sensitivity labels that do not auto-apply:
  - https://answers.microsoft.com/en-us/msoffice/forum/msoffice_o365admin-mso_security-mso_o365b/a-small-troubleshooting-guide-for-auto-applying/ffa60688-f500-4691-8fef-8cb0452c3faf?tm=1631607529198
- Co-Authoring for Encrypted Document:
  - Co-authoring on Microsoft Information Protection encrypted documents is now generally available - Microsoft Community Hub
- Co-Authoring for Mobile Devices:
  - Co-authoring for files with sensitivity labels is now generally available on Android and iOS devices - Microsoft Community Hub
- BLOG Post: Microsoft Information Protection Sensitivity Labelling Colours - Traffic Light System:
  - Microsoft Information Protection Sensitivity Labelling Traffic Light System - MSFT Compliance; Blogs, Vlogs, News & Announcements
- Adding Label Colours:
  - Manage sensitivity labels in Office apps - Microsoft Purview (compliance) | Microsoft Learn
- How to Troubleshoot Sensitivity Labels – Part 1:
  - How to troubleshoot sensitivity Labels – Part 1 - Microsoft Community Hub
- How to Troubleshoot Sensitivity Labels – Part 2:
  - How to troubleshoot sensitivity Labels – Part 2 - Microsoft Community Hub
- Custom configurations for the Azure Information Protection unified labeling client:
  - Custom configurations - Azure Information Protection unified labeling client | Microsoft Learn
- Identify Files & Emails That Have A Sensitivity Label:
  - Automatically apply a retention label to Microsoft 365 items - Microsoft Purview (compliance) | Microsoft Learn
- Auditing Labelling Activities:
  - Manage sensitivity labels in Office apps - Microsoft Purview (compliance) | Microsoft Learn
- Outlook: New Sensitivity Bar in Outlook on the Web:
  - https://www.microsoft.com/en-gb/microsoft-365/roadmap?filters=&searchterms=117578
- Microsoft Purview Information Protection in Microsoft 365 Apps | Office Apps on the Web can create PDFs that inherit the source files' sensitivity labels:
  - https://www.microsoft.com/en-gb/microsoft-365/roadmap?filters=&searchterms=117594

4.4 Container-Level, Groups & Sites Labelling

Container Level Labelling allows for the application of sensitivity labels to containers, such as SharePoint sites, Microsoft Teams, and Microsoft 365 Groups.
A recommendation I always suggest is to build out your Sensitivity Labels and Label Policies separate from your Groups & Sites' Labels and Policies. They are after all completely different configurations. Moreover, if you have the opportunity only provide access to the Groups & Sites Labels to administrators do so. This is due to the fact if a user is populated into a Groups & Sites Labelling Policy and has the right privileges on SharePoint or Teams, they have the right to remove the Label.

Here are the main points to understand about using M365 Groups and Sites Labelling:

- Data Classification: M365 Groups and Sites Labelling enables the classification and protection of data within Microsoft 365 Groups, SharePoint Sites, and related resources. It allows organisations to apply sensitivity labels to these groups and sites, ensuring appropriate protection of sensitive information.

- Sensitivity Labels: Administrators can define sensitivity labels that align with their organisation's data classification requirements. These labels can represent different levels of sensitivity or confidentiality, such as the examples above: Public, Internal, Confidential, or Highly Confidential. However, it is important to know, Groups and Sites Labelling should be designed separately from Email and File Labelling.

- Label Application: Sensitivity labels can be applied to M365 Groups and SharePoint Sites to classify the content within them. This ensures that the appropriate level of protection and access controls are applied to the data based on its sensitivity.

- Access Control: By assigning sensitivity labels to M365 Groups and Sites, administrators can control and restrict access to the content within these resources. Different sensitivity levels can have different permissions and restrictions, allowing organisations to enforce security and compliance policies.

- Collaboration and Sharing: Sensitivity labels help users understand the sensitivity of the content they are working with and guide them on the appropriate sharing and collaboration practices. Users can make informed decisions about sharing data based on the sensitivity labels assigned to the M365 Groups and Sites.

- Compliance and Auditing: Applying sensitivity labels to M365 Groups and Sites aids in meeting regulatory compliance requirements. It allows organisations to track and audit access, usage, and sharing activities related to sensitive data, supporting compliance with data protection regulations.

- Information Protection: M365 Groups and Sites Labelling enhances information protection by ensuring that sensitive information is properly classified, controlled, and protected. It helps prevent unauthorised access and reduces the risk of data breaches or accidental exposure.

As you can see, Groups and Sites labelling offers the opportunity to strengthen your security and compliance posture by enabling the addition of controls and content protection at the application layer of SharePoint, OneDrive, and Teams. It provides granular access rights for both users and guest users while ensuring visibility into unmanaged devices accessing the labelled content.

Groups & Sites Labelling is a feature that lets organisations apply labels to their Microsoft 365 groups and SharePoint sites. This can help you protect and manage your data better. However, this feature is not enabled by default. You need to do some extra steps to set it up.

Here's how:

- Sign in as a Compliance Administrator and go to the Microsoft 365 Compliance Centre.
- In the left navigation, click on Information Protection and then on Labels.
- Select the banner at the top that says, "Set up Container Level Labelling for your organisation". This means you need to enable the feature first.
- Click on Turn On and wait for the configuration to complete. This might take a few minutes.
- After that, you'll see another banner that says, "Sync labels with Groups & Sites". This means you need to make sure your labels are available for Groups & Sites.
- Click on the link in the banner and follow the instructions to sync your labels.
- When the sync is done, go back to the Labels page and check your labels. You should see a new option to apply them for Groups & Sites.
- Select the labels you want to use and configure the settings as you like.

That's it! You've successfully set up Groups & Sites Labelling for your organisation.

However, remember it might take up to 24 hours for the changes to take effect, so don't worry if you don't see them right away.

Note:

If you're having trouble with Groups & Sites Labelling, don't worry. I have a blog post that can help you out. It has all the steps and screenshots you need to set it up correctly.

- Enabling Container Level Sensitivity Labelling for Teams, Groups & Sites v2
  Enabling Container Level Sensitivity Labelling for Groups & Sites in Microsoft 365

4.4.1 Contributing Links:

- How to Configure Groups & Sites (Container-Level Labelling):
  - https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide#how-to-configure-groups-and-site-settings
- Configure a default sensitivity label for a SharePoint document library:
  - Configure a default sensitivity label for a SharePoint document library - Microsoft Purview (compliance) | Microsoft Learn
- Why Labelling Priority Matters
  - https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#label-priority-order-matters
- Mark Files as Sensitive by Default
  - Prevent guest access to files while DLP rules are applied - SharePoint in Microsoft 365 | Microsoft Learn
- How to Report Document Label Mismatch against an SPO Site Label (Tony Redmond)

  - Office365itpros/ReportDocumentSensitivityLabelMismatches.PS1 at master · 12Knocksinna/Office365itpros (github.com)

4.5 Teams Meeting Labelling

Microsoft has expanded the capabilities of its Information Protection Labelling by introducing protection for Microsoft Teams Meetings. This new feature allows organisations to apply sensitivity labels to Teams Meetings, providing enhanced control and protection for meetings that involve highly sensitive content or discussions.

With labelled Teams Meetings, you can enforce specific policies and restrictions to safeguard the confidentiality and integrity of sensitive discussions. For example, you can limit certain actions or permissions, such as file sharing, screen sharing, recording, or downloading of meeting content. This ensures that only authorised participants can access and interact with the meeting materials, reducing the risk of unauthorised dissemination or leakage of sensitive information.

Below is a high-level list of options available when labelling a Teams meeting.

- Who can bypass the lobby: Admins can manage the entry process and control who can directly join the meeting.
- Allow dial-in users to bypass the lobby: Configurable option to allow dial-in users to bypass the lobby.
- Who can present: Ensures that only authorised participants have the privilege to present during the meeting.
- Who can record: Control over who can record the meeting.
- Encryption for meeting video and audio: Option to enable encryption for video and audio streams in the meeting.
- Automatically record The ability to automatically record the meeting for archival purposes.
- Video watermark for screen sharing and camera streams: Enables the application of a watermark to screen sharing and camera streams to indicate sensitivity.
- Prevent or allow chat: Admins can decide whether participants can use the chat feature during the meeting.
- Prevent or allow copying chat to clipboard: Option to prevent or allow copying of chat to the clipboard.

These meeting settings, configurable through sensitivity labels, provide organisations with robust control and protection over their Teams Meetings, ensuring sensitive information is safeguarded and meeting content remains secure. Microsoft continues to enhance the features, and future updates will bring copy-prevention support for external meeting joiners and meeting chats on Safari, Firefox, and Mobile platforms.

Additionally, Microsoft has created a table of the features that can be enabled or disabled:

Feature	Setting	Location	Enforced
Allow cameras for attendees	On	Template	No
Allow mic for attendees	On	Template	No
Apply a watermark to everyone's video feed	On	Label	Yes
Apply a watermark to shared content	On	Label	Yes
End-to-end encryption	On	Label	Yes
Manage what attendees see	On	Template	Yes
Meeting chat	Only in meeting	Template	Yes
People dialling in can bypass the lobby	Off	Label	Yes
Prevent copying chat content to the clipboard	On	Label	Yes
Record automatically	(Disabled due to watermarking and encryption)	N/A	N/A
Who can bypass the lobby?	Only organizers and co-organizers	Label	Yes
Who can present	Only organizers and co-organizers	Label	Yes
Who can record	(Disabled due to watermarking and encryption)	N/A	N/A

4.5.1 Contributing Links:

- Configure Teams meetings with three tiers of protection.
  - Configure Teams meetings with three tiers of protection - Microsoft Teams | Microsoft Learn
- Configure Teams meetings with protection for highly sensitive data.
  - Configure Teams meetings with protection for highly sensitive data - Microsoft Teams | Microsoft Learn
- Microsoft Teams Premium - Overview for administrators.
  - Microsoft Teams Premium - Overview for administrators - Microsoft Teams | Microsoft Learn

4.6 Auto-Labelling Service-Side & Cloud Data Discovery & Labelling Enforcement (E5)

Service-Side Auto-Labelling is a feature that helps organisations protect and manage their data better. It allows admins to apply Sensitivity Labels to data automatically, based on the content of the data. This way, you don't have to label your data manually, and you can ensure that your labels are consistent across your organisation.

To use this feature, you need to define your Sensitive Information Types. These are the types of data that you want to label, such as credit card numbers, social security numbers, or confidential documents. As mentioned above in 3.1 you can either create your custom types that suit your business needs, or you can select from the default types that Microsoft provides. You can also combine multiple types to create more complex rules.

For example, you could create a custom type for project code names, such as Project Merger and Acquisition, Project Secret Product, etc. This type would match any data that contains these words. Or you could select a default type for UK National Insurance Number, which is a nine-digit code that identifies a person's eligibility for social security benefits in the UK. This type would match any data that contains a valid format of this code. Or you could combine multiple types of personal health information, such as medical record numbers, diagnosis, treatment, etc. This would match any data that contains any of these types.

Once you have defined your types, you need to configure the locations that you want the service to scan. These can be:

- SharePoint Sites
- OneDrive Accounts
- Exchange Mailboxes *(Data-in-Motion)*
- Teams' Chats

You can also specify the frequency of the scan, such as daily, weekly, or monthly.

For example, you could configure the service to scan:

- For a SharePoint Site that contains project documents and reports.
- For OneDrive, you could configure it to scan an account that belongs to a senior manager who handles sensitive data.
- For Exchange, you could configure it to scan a mailbox that receives customer feedback and complaints.
- For Teams, you could configure it to scan a chat that discusses confidential matters with external partners.

After the scan is complete, you will receive a report that shows you the results of the scan. The report will tell you where your sensitive data is located, what types of data it is, and what labels the service has applied or suggested for them. You can review the report and make any changes if needed. For example, you can remove labels from data that was labelled incorrectly, or you can apply labels to data that was not labelled by the service.

When you are satisfied with the report, you can turn on the enforcement option. This option will apply the labels to your data automatically, according to the rules that you have set up. This will help you protect your data with encryption, access control, retention policies, and other settings that are associated with your labels. For example, you could apply a label for confidential data to your project documents and reports. This label would encrypt the data and restrict access to authorised users only. Or you could apply a label for public data to your customer feedback and complaints. This label would not apply any protection and allow anyone to view or edit the data. Or you could apply a label for internal data to your Teams chat with external partners. This label would apply a watermark and prevent external sharing or printing of the data.

However, before you turn on the enforcement option, you should make sure that you test your Sensitive Information Types thoroughly. You should check that they are accurate and reliable and that they do not trigger false positives or negatives. You should also check that they do not conflict with each other or with other policies that you have in place. Furthermore, you should always verify the results of the scan before using them in an Auto-Labelling Policy.

This feature can help you save time and effort in labelling your data and ensure that your data is protected and managed according to your standards and or regulations.

4.6.1 Contributing Links:

- Service-side Auto-Labelling Playbook
  - Service Side Auto-labeling – Microsoft Purview Customer Experience Engineering (CxE)
- Service-Side Auto-Labelling:
  - Automatically apply a sensitivity label to content in Microsoft 365 – Microsoft 365 Compliance | Microsoft Docs

4.7 Labelling Policies

Publishing Sensitivity Labels is a vital step in making them available for use and ensuring consistent and effective information protection across your organisation. Therefore, once you have created your sensitivity labels, the next step is to publish them to ensure they are accessible to users and services within your organisation. By publishing the Sensitivity Labels, you enable their application to various items such as Office documents, emails, and other compatible content.

Within the Labelling Policies, your organisation can select which Labels should be mapped into a Policy and which users should see these labels. Additionally, Microsoft provides you with the ability to enhance the Policy configuration with the following:

- Users Must Provide a Justification to Remove a Label or Lower its Classification.
  - To remove a label or replace it with a lower-order priority label, users are required to justify.
  - The activity explorer can be utilised to review the changes made to labels and the accompanying justification text.

- Require Users to Apply a Label to their Emails and Documents.
  - Users must apply labels to documents before saving them or sending emails, provided that these items do not already have a label applied. This requirement ensures that appropriate sensitivity labels are consistently assigned to content within your organisation.

- Require Users to Apply a Label to their Power BI Content.

    - Users are obligated to apply labels to unlabelled content they create or edit in Power BI. This ensures that all content within Power BI is appropriately labelled for sensitivity, enhancing data classification and protection within the organisation.

- Provide Users with a Link to a Custom Help Page.
    - If your organisation has established a dedicated website aimed at assisting users in understanding how to utilise labels within your organisation, you can provide the URL for review.

- Inherit Labels From Attachments.
    - In the scenario where a label is initially applied to an email and subsequently an attachment with a higher priority label is added to the email, this setting ensures that the existing label is replaced by the label from the attachment. If multiple attachments with labels are added, the highest priority label among them will be applied. If the email does not already have a label, it will inherit the highest priority label from any attachments. There is also the option to configure a recommendation instead of automatically applying the label.

It's important to note that unlike retention labels, which are published to specific locations like all Exchange mailboxes, Sensitivity Labels are published to users or groups. This means that apps and services that support Sensitivity Labels can display them to the intended users and groups. Users will see the applied labels or have the option to apply the appropriate labels to their content, based on the permissions and configurations set by your organisation.

5 AIP Unified Labelling Client vs Built-In Labelling Client

The Unified Labelling Client and the Built-In Client are two options that your organisation can use to label and protect your data with Microsoft Information Protection. They both work with the same labels and policies that your organisation creates and manage in the Microsoft 365 compliance centre. They both provide a similar user experience and functionality for applying labels to your data. However, there are some differences between them that you should know.

The Unified Labelling Client is a separate client that you need to install on your Windows devices. It works with Office apps, such as Word, Excel, PowerPoint, and Outlook. It also works with File Explorer, where you can label and protect files and folders. The Unified Labelling Client has some features that the Built-In Client does not have, such as:

- The ability to scan and label files on your device.
- The ability to label files that are non-Microsoft.
- The ability to label files within Office Online.

The Built-In Client is a client that is already integrated into the Microsoft 365 apps ribbon. You do not need to install anything to use it. It works with Office apps, such as Word, Excel, PowerPoint, and Outlook. It also works with Office Online, where you can label and protect files in the browser. The Built-In Client has some features that the Unified Labelling Client does not have, such as:

- The ability to apply labels to Visio files.
- The ability to apply labels to co-authored files.
- The ability to apply labels based on sensitivity buttons.

- ➢ The ability to apply labels based on auto-labelling policies.

These are some of the differences between the Unified Labelling Client and the Built-In Client. You can choose the option that best suits your needs and preferences. You can also use both options together if you do not have any conflicts or issues with your labels and policies.
If you would like to learn more about the differences between the labelling clients, Albert Hoitingh has written an in-depth breakdown which is available in the contributing links below.

5.1 AIP Unified Labelling Client

Important Note
⊗ The AIP UL Client will be retired on April 11, 2024! ✓ Please ensure you have read and understood the 'Retirement Notification Link' below. ✓ Please make sure you are aware of the changes if you use this client.

You can continue to use the AIP UL Client; some customers will still require the use of the AIP UL Client. However, you will need to contact AIP2MIPGetHelp@microsoft.com for further information on supportability.

Should you need the Unified Labelling Client, the following information still stands. As stated above the main differences for the Unified Labelling Client are the capabilities to protect non-Microsoft files, for example, CAD, TXT, and JPEG, to name a few. This protection type is offered from Windows File Explorer by Right-Clicking on an item, and selecting, Classify & Protect, this then offers the user the ability to choose a Sensitivity Label.

There is something important your organisation should know about the Classify and Protect option. It has a feature that can cause problems for your information protection and data security. It is called 'Protect with Custom Permissions'. It lets the user choose their permissions for their data, instead of using the ones that you have set up with your labels and policies. This can lead to potential data exfiltration, which means your data can be leaked or stolen.

That is why I am recommending that you disable this feature. This way, your organisation can ensure that users follow your information protection and data security standards and that your data is safe and secure.

Here's how you can disable this feature:

- ➢ Go to the Microsoft 365 compliance centre.
- ➢ Click on Information Protection and then on Policies.
- ➢ Select the label policy that you want to edit.
- ➢ Click on Edit policy and then on Advanced settings.
- ➢ Uncheck the box that says, "Allow users to assign custom permissions using the Azure Information Protection client".
- ➢ Click on Save and then on Next.
- ➢ Review your changes and click on Submit.

That's it! You have successfully disabled the Protect with Custom Permissions feature. Now, your users will only be able to use the permissions that you have defined with your labels and policies.

5.2 Built-In Client

The Built-In Client is another option that you can use to label and protect your data with Microsoft Information Protection. It is a client that is already integrated into the Microsoft 365 apps ribbon, such as Word, Excel, PowerPoint, and Outlook. You do not need to install anything to use it. It works with Office apps and Office Online, where you can label and protect files in the browser.

The Built-in Client has undergone significant improvements in the past couple of years, with Microsoft introducing a range of new configuration options and features to enhance its flexibility and user-friendliness.

Notable additions to the Built-in Client that I am asked about the most:

- Co-authoring and AutoSave on Microsoft Information Protection-encrypted documents: Users can now collaborate on sensitivity-labelled documents in real time, making changes and saving them without compromising the protection or label settings.

- Client-based automatic and recommended labelling on Mac: The Built-in Client on Mac devices now supports automatic labelling or label recommendations, streamlining the labelling process and ensuring consistent and accurate data classification.

- Native support for variables and per-app content marking: Customisable content markings such as headers, footers, or watermarks can now be applied based on the app or label used with the Built-in Client.

- Sensitivity Buttons: Users can now apply labels using buttons, simplifying the label selection process, and making it faster and more convenient.

- Colours: Administrators can now apply colours within the Pureview Portal. Removing the need to use PowerShell.

- Auto-labelling Policies: Automation capabilities allow administrators to create policies that automatically apply labels to data based on specified conditions, ensuring correct and consistent data labelling.

These added features enable organisations to leverage the Built-in Client's capabilities for more efficient and effective data protection and labelling, adopting a stronger information protection posture and compliance adherence.

5.3 Contributing Links:

- Ignite 2022: 'New built-in labelling in Office makes it even easier to protect sensitive data:
  - Microsoft Purview Information Protection showcase of new capabilities at Ignite - Microsoft Community Hub
- Retirement notification for the Azure Information Protection Unified Labeling add-in for Office:
  - Retirement notification for the Azure Information Protection Unified Labeling add-in for Office - Microsoft Community Hub
- From Bolt-On to Build-In

  - From bold-on to build-in – Governance, Risk, Security and Compliance (alberthoitingh.com)
- Benefits of Deploying the Built-in Client:
  - The benefits of deploying built-in labeling within Microsoft 365 apps - Microsoft Tech Community
- Migrate the AIP Client to the Built-In Client:
  - Migrate the Azure Information Protection (AIP) add-in to Microsoft Purview Information Protection built-in labeling for Office apps - Microsoft Purview (compliance) | Microsoft Learn
- (Updated) Configuration Change: Azure Information Protection Add-in will be disabled by default for Office apps:
  - Message center - Microsoft 365 admin center
- Compare AIP Add-In with Built-In Labelling in M365 Apps:
  - CompareAIP2MIP - Microsoft Purview Customer Experience Engineering (CxE)
- Disable Custom Permissions in File Explorer:
  - Custom configurations - Azure Information Protection unified labeling client | Microsoft Docs
- Sensitivity Labelling Capabilities in Word, Excel & PowerPoint:

6 Microsoft Purview Information Protection scanner (Discover E3, Enforce E5) On-Premises Data Discovery & Labelling Enforcement

Microsoft Information Protection Scanner provides your organisation with the ability to automatically apply Sensitivity Labels based on data matched from a Sensitive Information Type.

You can use this feature for these locations:

- On-Premises SharePoint 2019, 2016, 2013 and 2010. However, be careful with SharePoint 2010, because it's in extended support only.
- UNC Paths that use SMB or NTFS Protocols.

For example, you could use this feature to scan a SharePoint Site that contains project documents and reports. Or you could use it to scan a UNC Path that stores customer data and invoices.

To use this feature, you need to create your labels and label policy in the Compliance Centre first. Then, you can run the scanner on your data and apply the labels automatically. This will help you protect your data with encryption, access control, retention policies, and other settings that are associated with your labels.

For example, you could apply a label for confidential data to your project documents and reports. This label would encrypt the data and restrict access to authorised users only. Or you could apply a label for public data to your customer data and invoices. This label would not apply any protection and allow anyone to view or edit the data.

Or you can run the scanner in Discovery Mode and get a report that shows you the information types detected in your data. This can help you understand your data better and decide what labels to use for them. This can be useful if you want to label your data before moving it to the cloud, especially if you have some regulatory requirements.

For example, you could run the scanner in Discovery Mode on your SharePoint site and find out that it contains credit card numbers, social security numbers, and project code names. Then, you could decide what labels to apply to these types of data.

6.1.1 Shared Experiences

My experience has shown that a good practice is to set up dedicated labels and label policies for testing or proof of concept. This way, you can change or remove them easily without affecting your users. Ensuring you can test your Sensitive Information Types carefully! Making sure they are accurate and reliable, and that they do not trigger false positives or negatives.

This is a feature that can help you save time and effort in labelling your data and ensure that your data is protected and managed according to your standards and industry regulations.

6.2 Contributing Links:

- Learn about the information protection scanner:
  - Learn about the Microsoft Purview Information Protection scanner – Microsoft Purview (compliance) | Microsoft Learn
- AIP Scanner Prerequisites:
  - Azure Information Protection (AIP) unified labeling scanner prerequisites | Microsoft Docs
- Deployment Guide:
  - https://docs.microsoft.com/en-us/azure/information-protection/deploy-aip-scanner-configure-install
- AIP Scanner Best Practises:
  - https://techcommunity.microsoft.com/t5/security-compliance-identity/best-practices-for-deploying-and-using-the-aip-ul-scanner/ba-p/1878168#reporting
- PowerShell Library:
  - PowerShell Gallery | AIPScannerConfig 1.1.92

7 Data Loss Prevention (E3 & E5)

Data Loss Prevention (DLP) is a critical component of any organisation’s information protection strategy. By implementing DLP Policies, your organisation can effectively identify, monitor, and protect sensitive information, reducing the risk of data leakage. This is achieved using advanced algorithms and techniques that can detect and classify sensitive data, allowing you to apply appropriate security measures to prevent unauthorised access or transmission.

DLP Policies can be customised to meet the specific needs of your organisation, allowing you to define what constitutes sensitive information and how it should be handled. This can include setting rules for data access, transmission, and storage, as well as defining actions to be taken in the event of a policy violation.

By implementing DLP, your organisation can strengthen its data protection capabilities, allowing it to grow and thrive while keeping its valuable data safe and secure. This not only helps to prevent accidental or intentional data leakage but also helps to maintain compliance with industry regulations and standards.

DLP offers many preventative patterns across the following areas:

- Workloads:
  - Exchange
  - Teams
  - SharePoint
  - OneDrive
  - Power BI
- Office Applications:
  - Word
  - Excel
  - PowerPoint
- Devices:
  - Windows 10 Devices
  - MacOS Devices
- Third-Party Cloud Applications (Defender for Cloud Apps):
  - Defender for Cloud Apps
    - DLP Integration/Extension
- On-Premises:
  - File Shares
  - SharePoint

7.1 M365 Data Loss Prevention (E3)

7.2 DLP Policies

DLP policies are the main way to configure and apply data loss prevention rules to the M365 workloads. You can create policies for specific workloads or all workloads. However, it is important to know that when selecting the M365 workloads where DLP can be configured, each workload will provide a different set of options within the rules. For example, having Exchange, SharePoint & OneDrive selected will provide fewer options than just having Exchange selected. As a result, I would always research the use cases for the organisation and then build out the DLP policies per location as required, maximising the configurable options available.

DLP policies can detect sensitive data based on two criteria:

- Sensitive Information Types: predefined or custom categories of data that have a specific format or pattern, such as credit card numbers, social security numbers, or bank account numbers. For example, you can create a DLP policy that blocks 25 or more credit card numbers from being shared with an external recipient via Exchange, SharePoint, OneDrive, and Teams. Furthermore, preventing uploads via browsers on Windows and macOS.

- Sensitivity Labels: labels that you can apply to documents or emails to classify their level of confidentiality, such as Highly Confidential, Confidential, or Public. For example, you can create a DLP policy that blocks the external sharing of documents that contain Highly Confidential financial information and have been labelled with a Sensitivity Label named Highly Confidential Internal. This way, you can prevent unauthorised disclosure of your organisation's financial data.

7.2.1 Policy Tips

Policy Tips are notifications that appear to users when they are about to violate a DLP policy. Policy Tips can help you educate your users on why certain data is sensitive and how to handle it properly. You can customise the text and actions of Policy Tips to suit your organisation's needs. For example, you can configure a Policy Tip that informs the user that they are trying to share a document that contains Highly Confidential financial information and advises them to remove the sensitive data or change the Sensitivity Label before sending it. You can also provide a link to your organisation's data protection policy or guidelines for more information.

7.2.2 Overrides

Overrides are exceptions that allow users to bypass a DLP policy under certain circumstances. You can enable overrides for specific policies or rules if you want to give your users some flexibility and trust. However, you should use overrides with **caution**, always enabling justifications and monitor their usage carefully. For example, you can allow overrides for a policy that blocks the external sharing of documents that contain Highly Confidential financial information if the user provides a valid business justification for doing so. This way, you can enable legitimate business scenarios while still enforcing data protection. Overrides will also generate an audit report that records the user's name, action, justification, and date and time.

7.2.3 Summary

M365 DLP is a powerful tool that can help you protect your organisation's sensitive data from unauthorised access or sharing. It allows you to create policies and rules that detect, and block data based on content, location, or user. It also provides features such as Policy Tips and Overrides that can help you educate your users and enable business scenarios. By using M365 DLP, you can enhance your data security and compliance while reducing data breaches and risks.

* **Note:**
Policy Tips Information. If you enable this configuration, make sure it does not reveal 'Tipping Off' information that may violate some regulations for regulated users.

7.2.4 Test Mode

It is highly advisable that when creating DLP Policies, the organisation does so in the configuration of Test It Out First. This will provide the ability to review the policy matches and assess the results, allowing for fine-tuning where required. Moreover, it will offer the chance to assess the policy's impact before turning it on. In addition, Microsoft offers the 'Show Policy Tips While in Test Mode' option. This can be an advantage when running a closed group Pilot as this will offer the chance to ensure when an item has been triggered, you can gain feedback on the results, guaranteeing the policy is picking up the correct entries.

7.2.5 Recent & New Features

Microsoft recently announced even more DLP features, detailed below:

7.2.5.1 DLP Policy Tips

DLP Policy Tips now support a richer set of DLP conditions (and corresponding exceptions), including the following:

- ➢ Content Contains Sensitive Information.

- Content contains a Sensitivity Label.
- Content is shared Internally/Externally.
- Sender is.
- The sender domain is.
- The sender is a member of
- Recipient is.
- The recipient domain is.
- The recipient is a member of
- The subject contains words.

In addition, DLP Policy Tips now support advanced classifiers like Trainable Classifiers, Exact Data Match (EDM), and Named Entities, as well as an Override feature that gives end users the ability to modify or override policies (if enabled in the DLP rule configuration). For example, you can use Trainable Classifiers to detect custom data types that are specific to your organisation, such as project names or product codes. You can use Exact Data Match to match data against a reference table that contains sensitive data, such as customer IDs or employee numbers. You can use Named Entities to identify specific people or organisations that are relevant to your data protection needs, such as executives or partners.

7.2.5.2 Content Contains Sensitivity Label

My standout new feature is the Content Contains Sensitivity Label. This has been a huge ask from many customers I have worked with in the past. Wanting to add a policy tip when detected can prevent the alert from being generated, reducing the reporting, and making the DLP Alerting and Reporting easier. For example, you can create a policy tip that warns the user that they are trying to share a document that has been labelled with a Sensitivity Label named Confidential External. You can advise them to change the label to Public or Internal before sharing it with external recipients. You can also provide a link to your organisation’s labelling policy or guidelines for more information.

7.2.6 Summary

The new DLP features, and Policy Tips offer more flexibility and functionality for data protection in M365 workloads. They allow you to create more granular and customised policies and rules that suit your organisation’s needs and scenarios. They also provide more feedback and guidance to your users on how to handle sensitive data properly. By using the new DLP features and Policy Tips, you can enhance your data security and compliance while reducing data breaches and risks.

7.3 Teams DLP (E3) & (E5)

Data Loss Prevention for Microsoft Teams can prevent the sharing of sensitive information within a Teams Chat or Channel, including Private Channels. A good example of this is blocking item(s) from being shared within a Teams conversation where External access has been enabled, or, where a Teams conversation has a Guest present. Along with blocking the item from being shared within the chat, administrators can apply a Policy Tip, this will display a message to the user who has triggered the rule allowing the organisation to educate their users on why this type of sensitive information cannot be shared.

Here are a couple of examples from Microsoft Docs:

For example: Protecting sensitive information in messages. Suppose that someone attempts to share sensitive information in a Teams Chat or Channel with guests (external users). If you have a DLP policy defined to prevent this, messages with sensitive information that are sent to external users are deleted.

For example: Protecting sensitive information in documents. Suppose that someone attempts to share a document with guests in a Microsoft Teams Channel or Chat, and the document contains sensitive information. If you have a DLP policy defined to prevent this, the document will not open for those users. Your DLP policy must include SharePoint and OneDrive for this level of protection to be in place. This is an example of DLP for SharePoint & OneDrive Files that show up in Microsoft Teams, and therefore requires that users are licensed for M365 DLP (included in M365 E3) but does not require users to be licensed for Office 365 Advanced Compliance.)

One thing to note: when a message containing potentially sensitive information is sent in Teams, the DLP engine needs a few seconds (typically 3 to 5 seconds) to detect and analyse the content of the message. During this time, the engine examines the message against the configured DLP policies to determine if any sensitive information is present and then enables DLP Actions within the rule.

If you require a setup video on how to create a DLP Policy, see my VLOG Post below in the contributing links.

Some frequently used Conditions in Team's Data Loss Prevention Policies are:

- Sender is.
- Recipient is.
- The sender domain is.
- The recipient domain is.

7.3.1 Contributing Links:

- Learn About DLP for Microsoft Teams
  - Learn about the default data loss prevention policy in Microsoft Teams (preview) - Microsoft 365 Compliance | Microsoft Docs
- Data Loss Prevention & Microsoft Teams
  - Data loss prevention and Microsoft Teams - Microsoft 365 Compliance | Microsoft Docs
- Announcing Public Preview of New Conditions in Teams DLP
  - Announcing Public Preview of New Conditions in Teams DLP - Microsoft Tech Community
- VLOG Post: Block Sensitive Information in Microsoft Teams with Data Loss Prevention – Overview
  - Block Sensitive Information in Microsoft Teams with Data Loss Prevention – Overview - MSFT Compliance; Blogs, Vlogs, News & Announcements

7.4 EndPoint DLP (E5)

EndPoint DLP is a feature that enables data protection on Windows and MacOS devices. It applies to data in use and at rest on the devices. EndPoint DLP can prevent organisational data from being leaked or stolen by blocking or auditing these actions, based on the content and sensitivity of the data. It can also notify you and the user when these actions are blocked or audited. This way, your organisation can keep your data safe and secure on your devices.

It can prevent data from being:

- Copied and Pasted: if a user tries to copy a document that contains sensitive information and paste it into another application, the action will be blocked, and the user will see a notification.

- Uploaded to Third-Party Cloud Services: if a user tries to upload a file that contains sensitive information to a cloud service that is not approved by the organisation, the action will be blocked, and the user will see a notification.

- Copied to USB Drives: if a user tries to copy a file that contains sensitive information to a USB drive, the action will be blocked, and the user will see a notification.

- Uploaded with non-Microsoft Browsers: if a user tries to upload a file that contains sensitive information using a browser that is not supported by the organisation, such as Chrome or Firefox, the action will be blocked, and the user will see a notification. Although, if your organisation uses Chrome or Firefox there are now detections enabled for these within the extensions listed below in the contributing links.

- Shared with External Domains: if a user tries to share a file that contains sensitive information with an external domain, such as outlook.com, gmail.com or yahoo.com, the action will be blocked, and the user will see a notification.

- Accessed by Unallowed Apps: if a user tries to open a file that contains sensitive information with an app that is not allowed by the organisation, such as Notepad ++ or Paint, the action will be blocked, and the user will see a notification.

DLP Rules can be used to configure the data protection settings. The options are:

- Audit: This will monitor and report the data activities, but not block them. This option can be used to assess the data landscape and plan the policies. For example, an organisation can use this option to audit their data activities for a period and identify the most common or risky scenarios that need to be addressed.

- Block: This will block the data activities and display a notification to the user. This option can be used to enforce the policies and prevent data loss. For example, an organisation can use this option to block data activities that involve high-risk information types, such as credit card numbers or social security numbers.

- Block with overrides: This will block the data activities but allow the user to override the block with a business justification. This option can be used to balance security and productivity. For example, an organisation can use this option to block their data activities that involve medium-risk information types, such as project code names or internal documents, but allow the user to override the block if they have a valid reason.

Before using EndPoint DLP, the devices need to be onboarded to the Compliance Centre. This will enable the service to scan and label the data on the devices. If the devices are enrolled in Defender for EndPoint, they will be onboarded automatically. Also, the devices need to be Windows 1809 or higher for EndPoint DLP to work. More information can be found in the Onboarding link below.

7.4.1 Contributing Links:

- Learn About Endpoint Data Loss Prevention
  - Learn about Endpoint data loss prevention - Microsoft Purview (compliance) | Microsoft Learn
- Get Started with EPDLP:
  - Get started with Microsoft 365 Endpoint data loss prevention - Microsoft 365 Compliance | Microsoft Docs
- Onboarding Devices:
  - Onboarding tools and methods for Windows 10 devices - Microsoft 365 Compliance | Microsoft Docs
- Using EPDLP:
  - Using Endpoint data loss prevention - Microsoft 365 Compliance | Microsoft Docs
- Plan for EPDLP:
  - Plan for data loss prevention - Microsoft 365 Compliance | Microsoft Docs

7.5 On-Premises Data Loss Prevention Scanner

Data Loss Prevention On-Premises Scanner is a feature that enables data protection for on-premises in SharePoint or File Shares. It allows organisations to scan and label their on-premises data-at-rest, based on the Sensitive Information Types and Sensitivity Labels that they use in Microsoft 365. This way, they can extend their data protection and security to their entire data estate, regardless of where it is located. They can also monitor and report their on-premises data activities and enforce their policies and prevent data loss. This feature can help organisations protect their organisation-critical data and comply with their regulatory requirements.

Here are some examples of how organisations can use this feature:

- An organisation that has confidential documents and reports stored on-premises in SharePoint. They want to protect these documents with a label that encrypts them and restricts access to authorised users only. They can use the Data Loss Prevention On-Premises Scanner to scan their SharePoint Site and apply the label automatically, based on the content of the documents.

- An organisation that has customer data and invoices stored on-premises in File Shares. They want to audit these files and report any activities that involve sensitive information, such as credit card numbers or social security numbers. They can use the Data Loss Prevention On-Premises Scanner to scan their File Shares and audit the files, based on any Sensitive Information Types that they have defined.

- An organisation that has internal documents and policies stored on-premises in SharePoint and File Shares. They want to move these documents to the cloud, but they need to ensure that they are labelled correctly before doing so. They can use the Data Loss Prevention On-Premises Scanner to scan their SharePoint and File Shares and label the documents, again based on the Sensitive Information Types and Sensitivity Labels that they have configured.

7.5.1 Contributing Links:

- Learn About Data Loss Prevention On-Premises Scanner
  - Learn about data loss prevention on-premises scanner - Microsoft Purview (compliance) | Microsoft Learn

7.6 DLP Collective Contributing Links:

I have created the links here a little differently from others due to the scale of DLP and the many links for polices rules, investigations, reports, and extensions. Therefore, I have segmented them into topical areas for ease of use.

Prepare	Plan for Data Loss Prevention
Prepare	Design a DLP Policy
Prepare	Data Loss Prevention policy reference
Implement	Create and Deploy Data Loss Prevention Policies
Implement	Configure EndPoint Data Loss Prevention Settings
Operational	Data Loss Prevention and Microsoft Teams
Operational	Using EndPoint Data Loss Prevention
Operational	Use the Data Loss Prevention On-Premises Repositories Location
Operational	Use Data Loss Prevention Policies for non-Microsoft Cloud Apps
Operational	Email Notifications and Show Policy Tips for DLP Policies
Operational	Data Loss Prevention Policy Tips Reference
Operational	Policies
Operational	View the Reports for Data Loss Prevention
Operational	Microsoft Purview Extension for Chrome
Operational	Microsoft Purview Extension for Firefox

7.7 Data Loss Prevention Alerting

To enhance the management of data and security concerns, DLP alerts and incidents are now accessible through the Defender Portal. To begin using this feature, it's important to activate them initially in the Purview Compliance Portal. DLP alerts and incidents have moved to the Defender Portal to provide a more collaborative space for data analysis and incident management.

The move offers several advantages that enhance information protection management:

Centralisation: Consolidating DLP alerts and incidents within the Defender Portal creates a unified platform for managing security-related issues. This streamlines operation by providing a single interface for monitoring and addressing data breaches or policy violations.

Collaboration: The Defender Portal provides a collaborative environment for teams to collectively analyse and address alerts. This fosters better communication and coordination among stakeholders, allowing for more efficient incident response.

Enhanced Features: The Defender Portal likely offers advanced features and tools for interacting with alerts and incidents. This could include capabilities such as adding comments, assigning ownership, and updating statuses, enabling more comprehensive and effective incident resolution.

Seamless Workflow: Having DLP alerts and incidents in the same portal as other security-related data enables a smoother workflow. Security professionals can seamlessly transition between different security tasks without switching between multiple platforms.

Improved Insights: By integrating DLP alerts and incidents into the Defender Portal, organisations can gain more comprehensive insights into their overall security landscape. This integration facilitates a holistic view of potential threats and vulnerabilities.

Unified Security Strategy: Bringing DLP alerts and incidents under the same umbrella as other security components align with a comprehensive security strategy. It ensures that data loss prevention is seamlessly integrated into broader security initiatives.

DLP encompasses various sections dedicated to overseeing and addressing alerts and incidents triggered by policy violations. These sections are as follows:

- Alerting Area in the Data Loss Prevention Blade within the Compliance Centre: This space allows you to review all alerts generated within your environment and take necessary actions, such as dismissing, resolving, or escalating them.

- Alerts and Incidents Area in the Microsoft Defender Portal: A newly introduced section that fosters collaborative data analysis. Here, you can access and engage with alerts within your environment in diverse ways, including adding comments, assigning owners, or updating statuses.

- Auditing Area in the Reports Blade within the Compliance Centre: This section provides an overview of DLP policy matches, incidents, false positives, and overrides in detail. Utilise this information to monitor and enhance the precision of your DLP policies.

7.7.1 DLP Alerting

Data Loss Prevention (DLP) has a dedicated alerting area within the Data Loss Prevention blade in the Compliance Centre. Although, with the new area within the Microsoft Defender Portal, Microsoft has provided a single area for DLP Alerts and Incidents. The new portal will display all the alerts that have occurred in the environment, providing the ability to triage and interact with the DLP incidents. The portals are:

- Data Loss Prevention Blade in the Compliance Centre: This portal shows the alerts by policy, severity, location, and status. You can also filter, sort, and export the alerts to a CSV file.

- Microsoft Defender Portal: This portal shows the alerts by policy, severity, location, user, and action. You can also filter, sort, and export the alerts to a CSV or PDF file. In addition, you can collaborate with other analysts by adding comments, tags, or feedback to the alerts.

7.7.2 DLP Auditing

Data Loss Prevention auditing is available from the Reports blade in the Compliance Centre. By navigating to Overview, you can see the following information:

- DLP Policy Matches: This report displays the matches made when a policy is in test mode. You can see the policy name, location, item details, and match details.

- DLP False Positives & Overrides: This report shows the overrides or false positive feedback provided by users or administrators. You can see the policy name, location, item details, override or false positive details, and justification.

- DLP Incidents: This report displays the incidents that have occurred at the item level. You can see the policy name, location, item details, incident details, and actions taken.

7.7.3 DLP Overview

Data Loss Prevention also provides some built-in details that you can access from the Data Loss Prevention blade in the Compliance Centre. These informational points are:

- Policy Health: This report shows the health status of your DLP policies based on their configuration and performance. You can see the policy name, status, severity, description, and recommendation.

- Policy Performance: This report shows the performance of your DLP policies based on their matches and incidents. You can see the policy name, matches, incidents, overrides, false positives, and trends.

- Policy Usage: This report shows the usage of your DLP policies based on their locations and users. You can see the policy name, locations, users, matches per location or user, and trend.

7.7.4 Contributing Links:

- Learn About Data Loss Prevention:
  - Learn about data loss prevention - Microsoft 365 Compliance | Microsoft Docs
- Plan for Data Loss Prevention:

  - Plan for data loss prevention - Microsoft 365 Compliance | Microsoft Docs
- Data Loss Prevention Policy Reference:
  - Data Loss Prevention policy reference - Microsoft 365 Compliance | Microsoft Docs
- Get Started with Data Loss Prevention:
  - Get started with the default DLP policy - Microsoft 365 Compliance | Microsoft Docs
- Policy Tips for Data Loss Prevention:
  - Send email notifications and show policy tips for DLP policies - Microsoft 365 Compliance | Microsoft Docs
- Policy Tips Reference:
  - Data Loss Prevention policy tips reference - Microsoft 365 Compliance | Microsoft Docs
- Alerts for Data Loss Prevention:
  - View the reports for data loss prevention - Microsoft 365 Compliance | Microsoft Docs
- VLOG Post: Block Sensitivity Labels with Data Loss Prevention – Overview
  - Block Sensitivity Labels with Data Loss Prevention - Overview - MSFT Compliance; Blogs, Vlogs, News & Announcements
- Expand DLP Policy Tips Functionality
  - Microsoft 365 Roadmap - New Releases - Updates | Microsoft 365

8 Information Barriers v2 (E5)[10]

Information Barriers allow your organisation to segment users into groups and control their; sharing and prevent conversations and calls with other users in the tenant. You can either block or allow communication within or outside of the same segment/group.

Information Barriers was originally designed for Financial Services regulation FINRA. It helps organisations avoid any potential conflicts of interest by preventing; Investment Bankers from communicating with Marketing and Equity Research departments to stop insider trading. I have deployed this solution not only for Banking but also for Education, Insurance, Legal and Retail.

To use Information Barriers, you need the following:

- Requires an E5 license for each user in a segment because the policies are bidirectional.

- Make sure prerequisites are met, such as having an E5 license for each user in a segment and enabling audit logging.

- Segment users in your organisation based on user account attributes, such as department, job title, location, etc.

- Create IB policies that define which segments can or cannot communicate or collaborate.

- Apply IB policies to your organisation.

- Configure Information Barriers on SharePoint and OneDrive.

[10] Information Barriers is part of Microsoft's Insider Risk Solutions Catalogue. I have added a reference here as this always comes up in information protection conversations.

- (Optional) Configure Information Barriers modes and user discoverability.

Microsoft has recently upgraded Information Barriers to a new architecture and substrate. This means that Information Barriers now support:

- Single-Segment and Multi-Segment configurations
- No longer relying on Exchange Online Address Book Policies

However, there are some limitations you should be aware of:

- Information Barriers does not support Exchange Online at present. If you need to block email communication between segments, you will need to use Mail Flow Rules.

8.1 Contributing Links:

- Information Barriers Overview
  - Information barriers - Microsoft Purview (compliance) | Microsoft Learn
- Learn about Information Barriers
  - https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers?view=o365-worldwide
- Get Started with Information Barriers
  - https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies?view=o365-worldwide
- Manage Information Barriers
  - Manage information barrier policies - Microsoft 365 Compliance | Microsoft Docs
- Information Barriers Attributes
  - Information barriers attributes - Microsoft 365 Compliance | Microsoft Docs
- Information Barriers Compliance Assistant
  - Information barriers compliance assistant (preview) - SharePoint in Microsoft 365 | Microsoft Learn
- Create an Information Barriers Policy Compliance Report
  - Create an information barriers policy compliance report - SharePoint in Microsoft 365 | Microsoft Learn
- Information Barriers for Teams
  - https://docs.microsoft.com/en-us/microsoftteams/information-barriers-in-teams
- Information Barriers for OneDrive
  - https://docs.microsoft.com/en-us/onedrive/information-barriers
- Information Barriers to SharePoint Online
  - Use information barriers with SharePoint - SharePoint in Microsoft 365 | Microsoft Docs

9 Multi-Geo

Multi-Geo enables organisations to store users' data-at-rest in a different region within their Microsoft 365 tenant, which may differ from the billing location or the location where the tenant was created. This capability is useful for meeting internal compliance needs, adhering to regional data sovereignty laws, or fulfilling regulatory obligations. By configuring Multi-Geo, users are assigned a regional code that determines the placement of their data in one of Microsoft's available in-country or in-region data centres. Multi-Geo is supported for workloads such as Teams, SharePoint, OneDrive, and Exchange Online.

Note:
You need an additional Add-On License to use Multi-Geo.

Here are some basic terms from Microsoft Docs to help you understand Multi-Geo:

- Tenant: Your organisation’s identity in Microsoft 365 with one or more domains, for example
  - Default URL https://contoso.sharepoint.com),
  - Multi-Geo SharePoint Online: HTTPS://<Tenant><GeoLocationCode>.sharepoint.com
  - Multi-Geo OneDrive for Business: HTTPS://<Tenant><GeoLocationCode>-my.sharepoint.com

- Geo Locations: The places where you can host data in Microsoft 365.

- Satellite Locations: The extra geo-locations that you set up to host data in your tenant. Multi-geo tenants span more than one geo-location, for example, North America and Europe.

- Preferred Data Location (PDL): Multi-Geo utilises an Azure AD Source Anchor, known as the Preferred Data Location (PDL) attribute to assign the regional code to associate users’ data, SharePoint Sites, and Teams Channels. You can change the PDL to any of the geo-locations enabled in your tenant.

9.1 Shared Experiences

Please note that changing the PDL for a user with a OneDrive site does not move their data automatically. See Move a OneDrive library to a different geo-location for more information. However, if they have an Exchange mailbox, the mailbox is moved to the new PDL automatically.

9.2 Contributing Links:

- Microsoft M365 Multi-Geo
  - Microsoft 365 Multi-Geo - Microsoft 365 Enterprise | Microsoft Docs
- Multi-Geo Capabilities for MS Teams
  - Multi-Geo Capabilities in Microsoft Teams - Microsoft 365 Enterprise | Microsoft Docs
- Multi-Geo Capabilities for OneDrive & SharePoint Online
  - Multi-Geo Capabilities in Microsoft Teams - Microsoft 365 Enterprise | Microsoft Docs
- Multi-Geo Capabilities for Exchange Online
  - Exchange Multi-Geo - Microsoft 365 Enterprise | Microsoft Docs

- Plan for Multi-Geo
  - Plan for Microsoft 365 Multi-Geo - Microsoft 365 Enterprise | Microsoft Docs
- Administering a Multi-Geo Environment
  - Administering a multi-geo environment - Microsoft 365 Enterprise | Microsoft Docs
- Multi-Geo User Experience
  - User experience in a multi-geo environment - Microsoft 365 Enterprise | Microsoft Docs
- Configure Multi-Geo
  - Microsoft 365 Multi-Geo tenant configuration - Microsoft 365 Enterprise | Microsoft Docs
- Configure the Preferred Data Location (PDL)
  - Azure AD Connect: Configure preferred data location for Microsoft 365 resources | Microsoft Docs
- Configure Search for Multi-Geo
  - Configure search for Microsoft 365 Multi-Geo - Microsoft 365 Enterprise | Microsoft Docs
- Moving to a new Datacentre Location with Multi-Geo
  - Moving core data to new Microsoft 365 datacenter geos - Microsoft 365 Enterprise | Microsoft Docs
- Where your data is stored
  - Microsoft 365 data locations - Microsoft 365 Enterprise | Microsoft Docs
- Azure Geographies
  - Choose the right Azure region for you | Microsoft Azure

10 Compliance Boundaries with Compliance Filters* (E3 & E5)

Compliance Boundaries is an eDiscovery solution based on RBAC Groups and Security Permissions Filtering. The RBAC Groups manage the M365 eDiscovery permissions of who can access a Compliance Boundary. The Security Permissions Filtering controls the content locations that can be searched within the configured Compliance Boundary. Combined, this enables the organisation to create the technical boundaries within which eDiscovery & Admins can:

- Conduct targeted searches for content.
- Preview search results.
- Export search results for investigation purposes.
- Perform soft deletes (Purge Items).

Countless multi-national organisations and Governments are required to incorporate eDiscovery to ensure Electronically Stored Information (ESI) is available as evidence in lawsuits and investigations. In addition, organisations should already have in place technical boundaries to control who can search for what data in which; regions, government agencies and in other cases organisation departments to protect company data. This is often due to internal compliance needs, regulatory requirements or data sovereignty laws that state each region, agency or organisation department must be implemented within technical walls to prevent cross-region, cross-agency and/or cross-departmental discovery of data. To accomplish this in M365, Microsoft offers Compliance Boundaries.

* **Note:**
Compliance Boundaries are an eDiscovery Premium feature which is covered by Discover & Respond. However, the question of; "Can I separate who can search for what data, within each department or a geo-region", always comes up when talking about Information Protection and organisational data. I feel these are a critical part of an organisational Information Protection strategy, hence including them for reference. If you would like to know more about Compliance Boundaries, you can visit my blog here: Microsoft Purview eDiscovery & Compliance Boundaries - MSFT Compliance; Blogs, Vlogs, News & Announcements

10.1 Contributing Links:

- Set Up Compliance Boundaries for eDiscovery Investigations.
  - Set up compliance boundaries for eDiscovery investigations – Microsoft Purview (compliance) | Microsoft Docs
- Configure Permissions Filtering for eDiscovery.
  - Configure permissions filtering for eDiscovery – Microsoft Purview (compliance) | Microsoft Docs
- Filterable Properties for the RecipientFilter Parameter on Exchange cmdlets
  - Filterable properties for the RecipientFilter parameter | Microsoft Docs
- New-ComplianceSecurityFilter
  - New-ComplianceSecurityFilter (ExchangePowerShell) | Microsoft Docs
  - https://docs.microsoft.com/en-gb/microsoft-365/compliance/sensitivity-labels-office-apps?view=o365-worldwide#sensitivity-label-capabilities-in-word-excel-and-powerpoint

11 Encryption Customer Key & Service-Level Encryption (E5)

Some regulators require organisations to encrypt their data in the Cloud, especially their most sensitive data. Microsoft offers different encryption solutions for this purpose such as:

- Microsoft Managed Key (MMK)
- Customer Key with Bring Your Own Key (BYOK)
- Hold Your Own Key (HYOK).

Each solution has its benefits and limitations, depending on the level of control and security needed. For example, BYOK allows organisations to use their own key in Azure Key Vault to encrypt data in the Cloud, and Double Key Encryption (DKE) adds an extra layer of protection by using two keys. HYOK, on the other hand, is more suitable for On-Premises Data that should not be shared or decrypted in the Cloud.

To learn more about these encryption solutions and how to use them in M365, please check out these links:

11.1 Contributing Links:

- Azure Information Protection Keys:
  - Your Azure Information Protection tenant key | Microsoft Docs
- M365 Encryption:
  - Encryption in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs

- DKE Option for Labelling:
  - Double Key Encryption (DKE) - Microsoft 365 Compliance | Microsoft Docs
- M365 Service Encryption:
  - Service Encryption - Microsoft 365 Compliance | Microsoft Docs
- Customer Lockbox Request
  - Customer Lockbox Requests - Microsoft 365 Compliance | Microsoft Docs

12 Availability Key (E5)

The Availability Key is a backup key that your organisation can create when you set up a Data Encryption Policy for your M365 data. A Data Encryption Policy allows you to use your own keys to encrypt your data at rest in the Cloud, giving you more control and ownership over your data. You can use different types of keys for different services and scenarios, such as Service Level Encryption and Information Protection (where applicable). For example, you can use a Customer Key with BYOK to encrypt your Exchange Online, SharePoint Online, and OneDrive for Business data, and use a different key to encrypt your Teams data. You can also use DKE to encrypt your most sensitive data with two keys, one of which is stored in Azure Key Vault and the other in a separate system.

However, using your own keys also comes with some risks and responsibilities. Your organisation needs to ensure that your keys are secure, accessible, and compliant with your policies and regulations. If your keys are lost, corrupted, or revoked, you *may* lose access to your encrypted data or compromise its security. To prevent this from happening, Microsoft requires you to create an Availability Key when you set up a Data Encryption Policy. The Availability Key is like the keys you use for Service Level Encryption and Information Protection, but you do not have direct access to it. Microsoft stores this key securely in M365 and uses it only in emergencies, such as when your keys in Azure Key Vault are compromised or inaccessible. For example, if your Azure subscription expires or is suspended, or if your key vault is deleted or disabled, Microsoft can use the Availability Key to decrypt your data and restore your access. Microsoft also periodically tests this key to ensure it is functional and reliable.

The Availability Key is not meant to replace or override your own keys. It is only a fallback option that Microsoft uses with your organisational consent and under strict conditions. You can monitor and audit the usage of the Availability Key through the M365 Compliance Centre or the Azure portal. You can also disable the Availability Key if you do not want Microsoft to use it, but this may increase the risk of losing access to your encrypted data. Therefore, it is recommended that you keep the Availability Key enabled and protect your own keys properly.

12.1 Contributing Links:

- Learn About Availability Key:
  - Learn about the availability key for Customer Key - Microsoft 365 Compliance | Microsoft Docs

13 Azure Key Vault

Azure Key Vault is a cloud-based service that allows you to store and manage your secrets in a centralised and secure way. Secrets are any data that you want to protect from unauthorised access, such as passwords, API keys, certificates, and encryption keys. You can use Azure Key Vault to create, store, and access your secrets using REST APIs or SDKs. You can also integrate Azure Key Vault with other Azure services, such as Azure Storage, Azure App Service, Azure Virtual Machines, and Azure SQL Database, to encrypt and decrypt your data using your secrets.

Azure Key Vault offers two service tiers that have different capabilities and pricing: Standard and Premium. The Standard tier encrypts your secrets using a software key that is generated and managed by Microsoft. The Premium tier uses hardware security modules (HSMs) to protect your secrets. HSMs are physical devices that provide high-level security and performance for your encryption operations. They are compliant with FIPS 140-2 Level 2 and Level 3 standards, which are widely recognised as the highest level of security for cryptographic modules. With the Premium tier, you can also import or generate your own HSM-protected keys, which gives you more control and ownership over your encryption keys.

Depending on your security and compliance requirements, you can choose the service tier that best suits your needs. For example, if you need to encrypt sensitive data that is subject to strict regulations, such as health or financial data, you may want to use the Premium tier with HSM-protected keys. If you need to encrypt less sensitive data that does not have specific regulatory requirements, you may opt for the Standard tier with software keys. You can also mix and match the service tiers for different types of secrets within the same key vault. For example, you can use the Premium tier for your encryption keys and the Standard tier for your passwords and certificates.

13.1 Contributing Links:

- Azure Key Vault:
  - Key Vault | Microsoft Azure
- Azure Key Vault Documentation
  - Azure Key Vault documentation | Microsoft Docs
- What is Azure Key Vault
  - What is Azure Key Vault? | Microsoft Docs
- Azure Key Vault Best Practises
  - Best practices for using Azure Key Vault | Microsoft Docs
- Azure Key Vault Pricing & Service Comparisons
  - Pricing Details –·Key Vault | Microsoft Azure

14 Customer Lock Box (E5)

Customer Lockbox is a feature that enhances the security and privacy of your organisational data in M365. It allows the organisation to control how Microsoft support engineers access your data when they need to troubleshoot or resolve an issue. By default, Microsoft support engineers have no access to your data and use a “Lockbox” process that requires multiple levels of approval within Microsoft. However, in some rare cases, they may need to request access to your data to perform a specific action, such as running a script or a diagnostic tool. In such cases, Customer Lockbox will notify an admin via email and the M365 Compliance Centre and ask them to review and approve or reject the request. They can also view the details of the request, such as the reason, the duration, and the scope of access. They can also audit the activities of the support engineer and revoke the access at any time.

Customer Lockbox is especially useful for organisations that are heavily regulated or that create and store highly sensitive data, such as health or financial data. It helps them comply with their policies and regulations and maintain their trust and confidence in Microsoft. Customer Lockbox is available for Exchange Online, SharePoint Online, OneDrive for Business, and Teams. It is included in M365 E5 and E5 Compliance plans, or as an add-on for other plans. To enable Customer Lockbox, you need to have the global administrator or compliance administrator role in M365.

14.1 Contributing Links:

- Customer Lock Box:
  - Office 365: What is Customer Lockbox and How to Enable it - TechNet Articles - United States (English) - TechNet Wiki (microsoft.com)

* Note:
I have provided the link for Customer Lockbox, what it does and how to request it. Customer Lockbox is an Insider Risk Solution and is enabled to Approve or Reject Microsoft Support from accessing organisational data. Therefore, the question of whether Microsoft can see my content, can Microsoft access my data, constantly comes up when talking about Information Protection and organisational data, hence why I have included it here for reference.

15 AIP Super User – Encryption & Decryption

The AIP Super User is a role that can remove encryption from any data that is protected by Azure Information Protection (AIP) which is now Microsoft Information Protection. AIP (MIP) is a service that allows users to classify and protect their data based on their sensitivity and confidentiality. Users can apply labels to their data that define the level of protection, such as encryption, access control, and visual markings. For example, a user can label a document as "Confidential" and encrypt it with a key that only allows authorised users to access it.

However, sometimes there may be situations where the encryption needs to be removed from the data, such as when the owner of the data leaves the organisation or changes roles, or when the data needs to be shared with external partners or regulators. In such cases, the AIP Super User can decrypt the data and remove the protection. The AIP Super User is a role that has full permission to access and modify any MIP-protected data, regardless of the label or the key. The AIP Super User can also audit and monitor the usage of MIP labels and keys across the organisation.

The AIP Super User role is not assigned to any user by default. It needs to be enabled and configured by the Global Administrator or the Security Administrator in the Azure portal. The administrator can assign the AIP Super User role to one or more users or groups, depending on their needs and policies. The administrator can also specify a scope for the AIP Super User role, such as a specific tenant, subscription, or resource group. The administrator should always review and update the AIP Super User role periodically to ensure that it is aligned with the organisation's security and compliance requirements.

* Note:
This feature must be enabled before it can be used.

15.1 Contributing Links:

- Enable AIP Super User
  - https://docs.microsoft.com/en-us/powershell/module/aipservice/enable-aipservicesuperuserfeature?view=azureipps
- AIP Super User Best Practices:
  - https://docs.microsoft.com/en-us/azure/information-protection/configure-super-users#security-best-practices-for-the-super-user-feature
- AIP Super User Configuration:

  - Configure super users for Azure Rights Management - AIP | Microsoft Docs

16 Defender for Cloud Apps & Information Protection Integration (E5)

Defender for Cloud Apps and MIP integration is a feature that enhances the protection and governance of your sensitive data in M365 and beyond. It allows you to use Sensitivity Labels, Sensitive Information Types, and DLP Policies to classify and protect your data based on its content and context. You can apply labels and policies to your data that define the level of protection, such as encryption, access control and inspection. For example, you can label a document as "Highly Confidential" and apply a policy that encrypts it with a key that only allows authorised users to access it.

Defender for Cloud Apps and MIP integration also allows you to extend the protection and governance of your data to third-party cloud solutions, such as Dropbox, Box, Google, and Amazon. You can connect these solutions to Defender for Cloud Apps and monitor their activities and risks. You can also prevent users from uploading or sharing data that has been labelled with a Sensitivity Label to these solutions or apply the same protection and policies to the data that is stored in these solutions. For example, you can prevent users from uploading a document that is labelled as "Highly Confidential" to Dropbox or encrypt the document with the same key if it is already stored in Dropbox.

In addition, Defender for Cloud Apps and MIP integration provides a retrospective encryption solution for data at rest in SharePoint Online (SPO) and OneDrive for Business (ODB). This means that you can encrypt your existing data in SPO and ODB with your own keys, without affecting the functionality or performance of these services. You can also decrypt your data if you need to access or share it. For example, you can encrypt all your documents in SPO with a Customer Key that you manage in Azure Key Vault and decrypt them when you need to edit or download them.

Defender for Cloud Apps and MIP integration also enables the investigation of files that are protected by Sensitivity Labels or DLP Policies. You can use the Defender for Cloud Apps portal to view all your classified data across M365 and third-party cloud solutions. You can also filter, sort, and export the data by various criteria, such as label, policy, owner, location, or risk level. You can also view the details of each file, such as its content, metadata, activity history, and protection status. This helps you gain visibility and insight into your sensitive data and ensure its compliance with your policies and regulations.

16.1 Contributing Links:

- MIP/AIP to CASB Integration:
  - Integrate Microsoft Information Protection with Defender for Cloud Apps | Microsoft Docs
- CASB Documentation Library:
  - Microsoft Defender for Cloud Apps documentation | Microsoft Docs
- CASB Data Protection Blog:
  - MCAS Data Protection Blog Series: Do I use MCAS or MIP? - Microsoft Tech Community

17 Microsoft Sentinel

Microsoft Sentinel is a cloud-native SIEM and SOAR solution that helps you detect, investigate, and respond to security and compliance threats across your hybrid environment. It leverages the power and scale of Azure and Microsoft 365 to collect and analyse data from various sources, such as devices, applications, servers, networks, and users. It also integrates with other Microsoft Security & Compliance solutions, such as:

- Microsoft Information Protection
- Microsoft Insider Risk Management
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Cloud App Security

The Data Connectors can provide a comprehensive view of your Security & Compliance posture and alerts.

With Microsoft Sentinel, you can use built-in or custom connectors to ingest data from different sources and then apply analytics rules or machine learning models to detect suspicious or malicious activities. You can also use Workbooks and Dashboards to visualise and monitor organisational data and alerts. You can use Kusto Query Language (KQL) to write queries or scripts to perform advanced data exploration and investigation. KQL is a powerful and expressive language that allows you to manipulate data in various ways, such as filtering, aggregating, joining, transforming, and charting. For example, you can use KQL to find all the failed logins from a specific IP address in the last 24 hours or to count the number of alerts by severity and category. Additionally, you can use KQL to find all Data Loss Prevention, Sensitivity Labelling, and Insider Risk activities, providing detailed logs on user activities.

Microsoft Sentinel also enables you to automate and orchestrate your response actions using playbooks. Playbooks are logic apps that can be triggered by alerts or events and execute a series of steps or tasks. You can use playbooks to perform common or repetitive actions, such as sending an email notification, creating a ticket, blocking an IP address, or running a script. You can also use playbooks to enrich your alerts with additional information from other sources, such as threat intelligence feeds or third-party tools. For example, you can use a playbook to query VirusTotal for the reputation of a file hash associated with an alert or to check if an email address is part of a phishing campaign.

Microsoft Sentinel helps you improve your security efficiency and effectiveness by providing a single solution that covers the entire threat lifecycle. It helps you reduce the complexity and cost of managing multiple security tools and platforms. It also helps you leverage the cloud scalability and innovation of Azure and Microsoft 365 to enhance your security capabilities and insights.

17.1 Shared Experiences

For MIP & DLP, I have developed robust workflows to monitor Sensitivity Labelling and Data Loss Prevention activities using Microsoft Power Automate and Azure Logic Apps. These workflows enable real-time alerting on critical events and can take proactive measures, such as revoking access to files from unauthorised users. For example, I have created a workflow that sends an email notification to the file owner and the compliance team whenever a file with a sensitivity label of

"Highly Confidential" is shared with an external user and revokes the sharing link to prevent data leakage.

Furthermore, I have implemented workflows to detect and investigate suspicious activities, such as unauthorised sharing of items, downgrading of sensitivity labels, unauthorised copying of items to external storage, and mass downloads by users. I can recreate users' steps when investigating Data Loss Prevention, run detections on the highest severity Sensitive Information Types in my organisation and where they are used and examine which users are adding files into a ZIP or RAR file in a potential attempt to evade Data Protection Policies. Additionally, I can also create the top 20 DLP Policy triggers and users in my organisation.

By leveraging these workflows, I have also created advanced analytics rules that generate alerts, triggering automated actions through Sentinel Playbooks. This seamless integration ensures that the Security Operations Centre (SOC) Teams receive timely detection alerts, allowing for immediate response and mitigation. For example, I have implemented workflows to detect and investigate suspicious activities, including unauthorised sharing of items, downgrading of sensitivity labels, and then emailing the items outbound, or unauthorised copying of these items to external storage, and mass downloads by users.

It is worth noting that there is vast potential for automation with Sentinel Playbooks, providing enhanced coverage and efficiency as needed. Through these comprehensive solutions and workflows, I can proactively monitor and protect sensitive data, mitigate risks, and strengthen our overall security posture.

17.2 Contributing Links:

- Microsoft Sentinel Documentation Library
  - Microsoft Sentinel documentation | Microsoft Learn
- Useful resources for working with Microsoft Sentinel
  - Useful resources when working with Microsoft Sentinel | Microsoft Learn
- What is Microsoft Sentinel
  - What is Microsoft Sentinel? | Microsoft Learn
- Microsoft Sentinel data connectors
  - Microsoft Sentinel data connectors | Microsoft Learn
- Kusto Query Language in Microsoft Sentinel
  - Kusto Query Language in Microsoft Sentinel | Microsoft Learn
- Rod Trent's Must Learn KQL Series
  - GitHub - rod-trent/MustLearnKQL: Code included as part of the MustLearnKQL blog series

18 Additional Links for Continued Information, Research, Updates and Announcements

What's New in Information Protection: these links provide a breakdown of everything that is newly released, I am providing this as most people are not aware it exists and it's a great resource to have. Additionally, I have included the new Microsoft Information Protection – One Stop Shop, which has all MIP information in a single link or library. This is a must-have link to bookmark!

18.1 Contributing Links:

- What's New in MIP:
  - What's New in Information Protection? - Microsoft Tech Community
- MIP One-Stop Shop:
  - Microsoft Information Protection in Microsoft 365 One Stop Shop Resource Page - Microsoft Tech Community
- M365 Compliance Licensing
  - microsoft-365-compliance-licensing-comparison.xlsx (live.com)
- Microsoft 365 Guidance for Security & Compliance
  - Microsoft 365 guidance for security & compliance - Service Descriptions | Microsoft Learn

19 About Me

I have been deploying Microsoft products for over 22 years. Most of this time has been supporting clients in designing, deploying, and migrating in Microsoft Exchange. This served as the foundation for my move to Microsoft Compliance, which has been my focus for the past 6 years. Many of my clients include some of the biggest names in Banking & Finance and Telecoms as well as clients across the UK & Global Legal industry, UK & EU Education and UK & EU Public Sector, e-Hospitals and Future Energy Cities in Arabia. This has seen me working with my clients to support their use of M365 both to actively support client processes and a compliant environment in line with the regulatory requirements of the relevant jurisdictions, especially data investigations and discovery.

I am a Microsoft Security MVP & Microsoft Security and Compliance Certified.

I Co-host the All-Things Microsoft 365 Compliance Podcast. If you love all things M365 compliance you can subscribe and follow us on the below:

- [All Things M365 Compliance - YouTube]
- https://open.spotify.com/show/17ylUnAOJ2INes5PNVQsmS?si=5f06a60b4d284fcc

MVP
Microsoft®
Most Valuable
Professional

20 Concluding This Kick-Start Guide

Thank you for reading this guide. I hope the information provided in this Kick-Start Guide has been beneficial to you, your company and/or even your customers.

In addition to this guide, I have guides for these solutions:

- Information Governance & Records Management
- Insider Risk Management & Communications Compliance
- eDiscovery

20.1 Important Notes:

1. The information laid out in this guide is not a step-by-step numbered translation of how to implement these solutions, it is simply the way I prefer to engage with organisations to:

    a) determine their requirements.
    b) determine their priorities with MIP & DLP.

2. I will try and make every effort to update this guide to new versions when the information within it changes. However, I cannot guarantee this will happen with the immediate effect of items changing. Additionally, all links are created and kept up to date by Microsoft.

3. Where advice is given always check the Microsoft official documentation and links which may or may not be provided, therefore, ensure the information is still up to date.