SC-400 Study Notes

[Implement information protection (25–30%) 2](#_Toc145579465)

[Create and manage sensitive info types 2](#_Toc145579466)

[Create and manage trainable classifiers 6](#_Toc145579467)

[Implement and manage sensitivity labels 9](#_Toc145579468)

[Design and implement encryption for email messages 13](#_Toc145579469)

[Implement DLP (15–20%) 15](#_Toc145579470)

[Create and configure DLP policies 15](#_Toc145579471)

[Implement and monitor Endpoint DLP 18](#_Toc145579472)

[Monitor and manage DLP activities 24](#_Toc145579473)

[Implement data lifecycle and records management (10–15%) 29](#_Toc145579474)

[Retain and delete data by using retention labels 29](#_Toc145579475)

[Manage data retention in Microsoft 365 workloads 33](#_Toc145579476)

[Implement Microsoft Purview records management 39](#_Toc145579477)

[Monitor and investigate data and activities by using Microsoft Purview (15–20%) 44](#_Toc145579478)

[Plan and manage regulatory requirements by using Microsoft Purview Compliance Manager 44](#_Toc145579479)

[Plan and manage eDiscovery and Content search 50](#_Toc145579480)

[Manage and analyze audit logs and reports in Microsoft Purview 58](#_Toc145579481)

[Manage insider and privacy risk in Microsoft 365 (15–20%) 63](#_Toc145579482)

[Implement and manage Microsoft Purview Communication Compliance 63](#_Toc145579483)

[Implement and manage Microsoft Purview Insider Risk Management 65](#_Toc145579484)

[Implement and manage Microsoft Purview Information Barriers (IBs) 69](#_Toc145579485)

[Implement and manage privacy requirements by using Microsoft Priva 73](#_Toc145579486)

[Diagrams & Notes 78](#_Toc145579487)

# Implement information protection (25–30%)

## Create and manage sensitive info types

### Identify sensitive information requirements for an organization's data

* **Definition**: Sensitive information refers to data that requires special protection due to its importance or potential harm if exposed.
* **Identification Process**:
  + **Data Inventory**: Create a comprehensive inventory of all data assets within the organization.
  + **Data Classification**: Categorize data based on its sensitivity, such as public, internal, confidential, or highly confidential.
* **Regulatory Compliance**:
  + Identify relevant data protection regulations (e.g., GDPR, HIPAA, CCPA).
  + Determine which data falls under regulatory purview.
* **Data Owner and Stakeholder Involvement**:
  + Involve business units and data owners to understand their data requirements and sensitivity.
* **Risk Assessment**:
  + Evaluate the potential risks associated with different data types.
  + Consider factors like data value, impact of loss, and likelihood of exposure.
* **Data Sensitivity Labels**:
  + Develop a labeling system to mark sensitive data.
  + Labels may include "Public," "Internal Use Only," "Confidential," etc.
* **Data Mapping**:
  + Map data flows to understand how sensitive data moves within the organization.
  + Identify data repositories and access points.
* **Data Retention Policies**:
  + Determine how long sensitive data should be retained.
  + Align with legal requirements and business needs.
* **Data Handling Procedures**:
  + Establish procedures for handling, storing, and transmitting sensitive data securely.
  + Encrypt, anonymize, or pseudonymize data as needed.
* **Security Controls**:
  + Implement access controls, encryption, and authentication mechanisms.
  + Regularly monitor and audit access to sensitive data.
* **Data Incident Response Plan**:
  + Develop a plan to respond to data breaches or incidents involving sensitive information.
  + Ensure compliance with breach notification requirements.
* **User Training and Awareness**:
  + Educate employees on the importance of handling sensitive data securely.
  + Conduct regular training sessions and awareness campaigns.
* **Data Destruction**:
  + Establish procedures for secure data disposal when it's no longer needed.
  + Consider shredding physical documents and securely wiping digital data.
* **Data Masking and Redaction**:
  + Use techniques like data masking and redaction to protect sensitive information in reports or documents.
* **Monitoring and Auditing**:
  + Implement continuous monitoring and auditing to detect unauthorized access or data breaches.
* **Documentation**:
  + Maintain clear documentation of data sensitivity requirements and controls in place.
* **Review and Update**:
  + Regularly review and update sensitive information requirements to adapt to evolving risks and regulations.
* **Privacy Impact Assessments (PIAs)**:
  + Conduct PIAs for new projects involving sensitive data to assess privacy risks.
* **Third-Party Data Handling**:
  + Assess how third-party vendors handle sensitive data and ensure compliance with your organization's requirements.
* **Incident Reporting**:
  + Establish a clear process for reporting and documenting data security incidents.

### Translate sensitive information requirements into built-in or custom sensitive info types

* **Sensitive Info Types**:
  + Sensitive info types are predefined or custom patterns that identify sensitive data.
  + Examples include credit card numbers, social security numbers, and custom-defined patterns.
* **Built-in Sensitive Info Types**:
  + Microsoft 365 provides a library of built-in sensitive info types.
  + These cover common data types like email addresses, phone numbers, and financial information.
* **Custom Sensitive Info Types**:
  + Create custom sensitive info types for unique organizational requirements.
  + Use regular expressions, keywords, or dictionaries to define custom patterns.
* **Identifying Requirements**:
  + Work with stakeholders to understand specific data sensitivity requirements.
  + Determine what data elements need protection.
* **Mapping to Sensitive Info Types**:
  + Match sensitive data requirements to appropriate built-in or custom sensitive info types.
* **Examples**:
  + If protecting patient information, map to "Medical Records" sensitive info type.
  + For proprietary product names, create a custom info type.
* **Regular Expressions**:
  + Custom sensitive info types often use regular expressions for precise pattern matching.
  + Define regex patterns for things like credit card numbers or employee IDs.
* **Keyword Dictionaries**:
  + Create custom info types using keyword dictionaries for lists of sensitive terms.
  + Useful for identifying project codes, product names, or other specific terms.
* **Testing and Validation**:
  + Test sensitive info types to ensure they accurately identify sensitive data.
  + Validate against sample data to avoid false positives or negatives.
* **Integration with DLP**:
  + Integrate sensitive info types with Data Loss Prevention (DLP) policies.
  + Enforce actions like blocking, alerting, or encrypting when sensitive data is detected.
* **Continuous Monitoring**:
  + Regularly review and update sensitive info types to adapt to changing data requirements.
* **Data Classification Labels**:
  + Combine sensitive info types with data classification labels for comprehensive data protection.
* **User Education**:
  + Train employees on the use of sensitive info types and data handling best practices.
* **Compliance Requirements**:
  + Ensure that sensitive info types align with regulatory compliance needs (e.g., GDPR, HIPAA).
* **Documentation**:
  + Maintain documentation of how sensitive info types are configured and used.

### Create and manage custom sensitive info types

* **Custom Sensitive Info Types**:
  + Custom sensitive info types are used to identify unique data patterns specific to an organization.
* **Creation Process**:
  + Access Microsoft 365 Compliance Center.
  + Under "Classifications," create a new custom sensitive info type.
* **Pattern Definitions**:
  + Define custom patterns using regular expressions, keywords, or dictionaries.
  + Examples: Custom project codes, product names, proprietary terms.
* **Testing and Validation**:
  + Test custom info types with sample data to ensure accurate identification.
  + Refine patterns to minimize false positives or negatives.
* **Integration with DLP**:
  + Integrate custom info types with Data Loss Prevention (DLP) policies.
  + Apply actions (e.g., block, alert) when custom-sensitive data is detected.
* **Continuous Management**:
  + Regularly review and update custom info types to adapt to evolving data needs.
* **Data Classification Labels**:
  + Combine custom info types with data classification labels for comprehensive data protection.
* **User Education**:
  + Train employees on using custom info types and data handling best practices.
* **Compliance Requirements**:
  + Ensure custom info types align with regulatory compliance needs (e.g., GDPR, HIPAA).
* **Documentation**:
  + Maintain documentation on how custom-sensitive info types are configured and used.

### Create and manage exact data match (EDM) classifiers

* **Exact Data Match (EDM)**:
  + EDM is a feature in Microsoft 365 that helps identify exact matches of sensitive data.
* **Creating EDM Classifiers**:
  + Go to the Microsoft 365 Compliance Center.
  + Under "Classifications," create a new EDM classifier.
  + Define the sensitive data pattern to match (e.g., social security numbers).
* **Pattern Definition**:
  + Use regular expressions or predefined patterns to specify data to match.
  + Custom patterns allow precise identification (e.g., specific formats of IDs).
* **Testing Classifiers**:
  + Validate classifiers against sample data to ensure accurate matching.
  + Adjust patterns to minimize false positives and negatives.
* **Applying Classifiers**:
  + Apply EDM classifiers to content locations like Exchange, SharePoint, or OneDrive.
  + Use them in Data Loss Prevention (DLP) policies.
* **Managing Classifiers**:
  + Regularly review and update classifiers to adapt to changing data needs.
  + Delete obsolete classifiers to maintain efficiency.
* **Integration with DLP**:
  + Combine EDM classifiers with DLP policies to take actions (e.g., block, notify) when matches are found.
* **User Education**:
  + Educate users about the use of EDM classifiers and their role in data protection.
* **Reporting and Monitoring**:
  + Monitor EDM matches through reports in the Compliance Center.
  + Investigate and remediate incidents as necessary.
* **Compliance Requirements**:
  + Ensure that EDM classifiers align with regulatory compliance requirements (e.g., GDPR, HIPAA).
* **Documentation**:
  + Maintain documentation on how EDM classifiers are configured and applied.

### Implement document fingerprinting

* **Document Fingerprinting**:
  + Document fingerprinting is a data protection technique that identifies and tracks sensitive documents.
* **Implementation Steps**:
  + **Access Microsoft 365 Compliance Center**:
    - Go to the Microsoft 365 Compliance Center.
  + **Create a New Document Fingerprinting Policy**:
    - Under "Classification," create a new document fingerprinting policy.
  + **Define Fingerprinting Rules**:
    - Specify criteria for identifying sensitive documents, such as keywords, phrases, or patterns.
  + **Assign the Policy**:
    - Assign the policy to specific content locations (e.g., SharePoint, OneDrive, Exchange).
  + **Monitoring and Alerts**:
    - Monitor for matches and receive alerts when sensitive documents are detected.
  + **Remediation Actions**:
    - Define actions to take when sensitive documents are found (e.g., block, notify).
* **Customization**:
  + Tailor fingerprinting rules to match organization-specific sensitive data.
* **Integration with DLP**:
  + Integrate document fingerprinting with Data Loss Prevention (DLP) policies for enhanced protection.
* **Continuous Monitoring**:
  + Regularly review and update fingerprinting policies to adapt to changing data needs.
* **Compliance Requirements**:
  + Ensure document fingerprinting aligns with regulatory compliance (e.g., GDPR, HIPAA).
* **Documentation**:
  + Maintain documentation on how document fingerprinting policies are configured and used.

## Create and manage trainable classifiers

### Identify when to use trainable classifiers

* **Trainable Classifiers**:
  + Trainable classifiers are machine learning models that classify and identify specific content in Microsoft 365 services.
* **Use Cases**:
  + **Custom Data Types**: Use trainable classifiers when dealing with custom data types or unique content that built-in classifiers cannot identify.
  + **Industry-Specific Data**: Apply trainable classifiers for industry-specific content, such as medical records in healthcare or legal documents in the legal sector.
  + **Unique Keywords or Phrases**: When content includes unique keywords or phrases important to your organization's data protection.
  + **Sensitive Data Variability**: Trainable classifiers are valuable when sensitive data varies in format or structure.
  + **Adaptive Needs**: Use when data sensitivity and classification requirements evolve over time, and you need a dynamic solution.
* **Training Process**:
  + Train the classifier by providing labeled examples of both positive and negative matches.
* **Continuous Refinement**:
  + Regularly refine and update trainable classifiers to improve accuracy and adapt to changing data patterns.
* **Integration with DLP**:
  + Integrate trainable classifiers with Data Loss Prevention (DLP) policies to enforce actions on identified content.
* **Compliance Requirements**:
  + Use trainable classifiers to meet regulatory compliance needs (e.g., GDPR, HIPAA) for unique data types.
* **Documentation**:
  + Maintain documentation of when and how trainable classifiers are used in your organization.

### Design and create a trainable classifier

* **Trainable Classifier**:
  + A trainable classifier is a machine learning model used to classify and identify specific content in Microsoft 365 services.
* **Designing a Classifier**:
  + Define the objective: Determine what specific content or data type you want to classify (e.g., sensitive documents, industry-specific terms).
* **Data Collection**:
  + Gather a dataset with labeled examples:
    - Positive examples: Content that matches the classification criteria.
    - Negative examples: Content that doesn't match the criteria.
* **Training Process**:
  + Access Microsoft 365 Compliance Center.
  + Create a trainable classifier.
  + Upload the labeled dataset.
  + Start the training process.
* **Refinement**:
  + Review the classifier's performance.
  + Refine the model by providing additional labeled data or adjusting parameters.
* **Testing and Validation**:
  + Validate the classifier's accuracy by running it against sample data.
  + Fine-tune as needed to minimize false positives and negatives.
* **Integration with DLP**:
  + Integrate the trained classifier with Data Loss Prevention (DLP) policies for enforcement.
* **Continuous Improvement**:
  + Regularly update and retrain the classifier to adapt to changing data patterns.
* **Documentation**:
  + Maintain documentation on the classifier's purpose, training process, and performance.

### Test a trainable classifier

* **Testing a Trainable Classifier**:
  + Testing a trainable classifier ensures its accuracy and effectiveness in identifying specific content.
* **Steps to Test**:
  + **Select Test Data**: Choose a representative dataset with a mix of content that should and should not match the classifier criteria.
  + **Run Classifier**: Apply the trainable classifier to the selected test data.
  + **Review Results**: Examine the results to identify:
    - True Positives: Content correctly identified as matching.
    - True Negatives: Content correctly identified as not matching.
    - False Positives: Content incorrectly identified as matching.
    - False Negatives: Content incorrectly identified as not matching.
  + **Calculate Metrics**: Calculate accuracy, precision, recall, and F1-score to evaluate the classifier's performance.
  + **Refinement**: Based on test results, refine the classifier to improve accuracy and reduce false positives or negatives.
* **Continuous Testing**:
  + Regularly test the classifier with new data to ensure ongoing accuracy.
* **Integration with DLP**:
  + Integrate the trained classifier with Data Loss Prevention (DLP) policies for real-time content evaluation and enforcement.
* **Documentation**:
  + Maintain records of testing procedures, results, and any classifier adjustments made.

### Retrain a trainable classifier

* **Retraining a Trainable Classifier**:
  + Periodic retraining is essential to maintain the accuracy and effectiveness of a trainable classifier.
* **Reasons for Retraining**:
  + Data Drift: As data patterns change over time, the classifier may become less accurate.
  + Improved Performance: Retraining allows you to refine and enhance the model's accuracy.
  + Evolving Criteria: Adapt the classifier to new criteria or requirements.
* **Steps to Retrain**:
  + **Data Collection**: Gather a new dataset with labeled examples.
  + **Upload Data**: Access the Microsoft 365 Compliance Center and upload the new dataset.
  + **Retraining**: Initiate the retraining process, allowing the model to learn from the updated data.
  + **Testing**: After retraining, test the classifier's performance to ensure accuracy.
  + **Deployment**: Apply the updated classifier to relevant content locations or policies.
* **Frequency**:
  + Retraining frequency depends on the rate of data change. It can range from quarterly to annually.
* **Continuous Monitoring**:
  + Continuously monitor the classifier's performance to identify when retraining is necessary.
* **Documentation**:
  + Maintain documentation of retraining schedules, processes, and outcomes.

## Implement and manage sensitivity labels

### Implement roles and permissions for administering sensitivity labels

* **Roles and Permissions**:
  + Define specific roles and permissions to manage sensitivity labels effectively.
* **Administrator Roles**:
  + Assign roles such as "Sensitivity Label Administrator" to individuals responsible for label management.
* **Assign Permissions**:
  + Grant permissions based on the responsibilities of label administrators.
  + Assign permissions to create, edit, publish, and apply sensitivity labels.
* **Role Groups**:
  + Organize administrators into role groups for easy permission assignment.
* **Azure AD Roles**:
  + Utilize Azure Active Directory (Azure AD) roles for sensitivity label administration.
* **Least Privilege Principle**:
  + Follow the principle of least privilege, granting only necessary permissions to each administrator.
* **Label Management Portal**:
  + Use the Microsoft 365 Compliance Center or Azure Portal for sensitivity label administration.
* **Testing and Validation**:
  + Test sensitivity labels in a controlled environment to ensure they align with organizational requirements.
* **Documentation**:
  + Maintain documentation of roles, permissions, and responsibilities for sensitivity label administration.

### Define and create sensitivity labels

* **Sensitivity Labels**:
  + Sensitivity labels help classify and protect data based on its sensitivity level.
* **Definition**:
  + Define the purpose and criteria for sensitivity labels, such as "Confidential" or "Internal Use."
* **Label Components**:
  + Configure label components:
    - Name: Label identifier.
    - Description: Explanation of label purpose.
    - Visual Markings: Icons, watermarks, or colors to signify label.
    - Protection Settings: Encryption, access controls, and data loss prevention (DLP) policies.
* **Label Templates**:
  + Create label templates to apply consistent settings across multiple labels.
* **Permissions and Labeling Policies**:
  + Specify who can assign labels and under what conditions.
* **Automated Labeling**:
  + Use auto-labeling policies to apply labels automatically based on content inspection.
* **Testing and Validation**:
  + Validate labels on sample data to ensure they correctly identify and protect sensitive content.
* **Integration with DLP**:
  + Integrate sensitivity labels with DLP policies to enforce actions on labeled content.
* **Deployment**:
  + Deploy labels to content locations like SharePoint, OneDrive, Exchange, and Teams.
* **User Training**:
  + Educate users on the meaning and proper use of sensitivity labels.
* **Documentation**:
  + Maintain documentation on label definitions, settings, and deployment.

### Configure and manage sensitivity label policies

* **Sensitivity Label Policies**:
  + Sensitivity label policies define how labels are applied and enforced across an organization's data.
* **Configuration Steps**:
  + **Access Settings**: Go to the Microsoft 365 Compliance Center or Azure Portal.
  + **Create Label Policy**: Define a new label policy, specifying:
    - Label assignments: Who gets which labels.
    - Label behavior: How labels affect data (e.g., encryption, access controls).
  + **Apply to Locations**: Choose where the label policy applies (e.g., SharePoint, OneDrive, Exchange).
  + **Assign to Users or Groups**: Specify who the policy applies to (users, groups).
* **Scope and Priority**:
  + Determine the scope and priority of label policies to avoid conflicts and ensure consistency.
* **Auto-Labeling Policies**:
  + Implement auto-labeling policies to automatically apply labels based on content inspection.
* **Testing and Validation**:
  + Test label policies on sample data to ensure they function as intended.
* **Monitoring and Reporting**:
  + Monitor label policy compliance and use reports to track labeling activities.
* **Revocation and Updates**:
  + Configure label policies to revoke or update labels when needed.
* **Documentation**:
  + Maintain documentation of label policies, configurations, and updates

### Configure auto-labeling policies for sensitivity labels

* **Sensitivity Label Policies**:
  + Sensitivity label policies define how labels are applied and enforced across an organization's data.
* **Configuration Steps**:
  + **Access Settings**: Go to the Microsoft 365 Compliance Center or Azure Portal.
  + **Create Label Policy**: Define a new label policy, specifying:
    - Label assignments: Who gets which labels.
    - Label behavior: How labels affect data (e.g., encryption, access controls).
  + **Apply to Locations**: Choose where the label policy applies (e.g., SharePoint, OneDrive, Exchange).
  + **Assign to Users or Groups**: Specify who the policy applies to (users, groups).
* **Scope and Priority**:
  + Determine the scope and priority of label policies to avoid conflicts and ensure consistency.
* **Auto-Labeling Policies**:
  + Implement auto-labeling policies to automatically apply labels based on content inspection.
* **Testing and Validation**:
  + Test label policies on sample data to ensure they function as intended.
* **Monitoring and Reporting**:
  + Monitor label policy compliance and use reports to track labeling activities.
* **Revocation and Updates**:
  + Configure label policies to revoke or update labels when needed.
* **Documentation**:
  + Maintain documentation of label policies, configurations, and updates.

### Monitor data classification and label usage by using Content explorer, Activity explorer, and audit search

* **Monitoring Data Classification**:
  + Use Content Explorer, Activity Explorer, and Audit Search to track data classification and label usage in Microsoft 365.
* **Content Explorer**:
  + Content Explorer allows you to view and search for labeled content.
  + You can filter by sensitivity label, content location, and more.
  + It helps identify where labeled data is stored.
* **Activity Explorer**:
  + Activity Explorer tracks user and administrator actions related to labeled content.
  + You can monitor label changes, access, sharing, and more.
  + Helps you understand how labels are used and who interacts with labeled data.
* **Audit Search**:
  + Audit Search enables detailed investigation of labeled content activities.
  + You can create custom audit log queries to track specific label-related events.
  + Useful for in-depth analysis and compliance reporting.
* **Continuous Monitoring**:
  + Regularly use these tools to monitor data classification and label usage.
  + Identify trends, anomalies, or potential security incidents.
* **Compliance and Reporting**:
  + Leverage the information from these tools for compliance reporting and auditing purposes.
* **User Training**:
  + Educate users on how to properly use and handle labeled data.
* **Documentation**:
  + Maintain records of data classification monitoring activities for compliance and auditing purposes.

### Apply bulk classification to on-premises data by using the Microsoft Purview Information Protection scanner

* **Bulk Classification with Purview Scanner**:
  + Microsoft Purview Information Protection scanner automates the classification of on-premises data.
* **Steps to Apply Bulk Classification**:
  + **Install Purview Scanner**:
    - Install and configure the Microsoft Purview Information Protection scanner on your on-premises systems.
  + **Configuration**:
    - Configure the scanner settings, including data sources, scan frequency, and target repositories.
  + **Data Scanning**:
    - The scanner scans on-premises data repositories, such as file servers and SharePoint.
  + **Classification Rules**:
    - Define classification rules based on sensitivity labels or content inspection criteria.
  + **Classification Results**:
    - Review the results of the scanning process to see how data has been classified.
  + **Auto-Classification**:
    - Automate the application of sensitivity labels based on defined rules.
* **Continuous Scanning**:
  + Schedule regular scans to ensure newly added or modified data is also classified.
* **Integration with Sensitivity Labels**:
  + Align the scanner with your sensitivity label configuration for consistency.
* **Monitoring and Reporting**:
  + Monitor the scanner's activity and generate reports on data classification.
* **Documentation**:
  + Maintain documentation on scanner configurations, rules, and scanning results for auditing and compliance purposes.

### Manage protection settings and marking for applied sensitivity labels

* **Protection Settings**:
  + Sensitivity labels can enforce protection settings on labeled content.
* **Configuration**:
  + Define protection settings like encryption, access controls, and data loss prevention (DLP) policies within sensitivity labels.
* **Label Assignment**:
  + Apply sensitivity labels to content based on label policies, manual assignment, or auto-labeling.
* **Protection Enforcement**:
  + Once applied, labels enforce protection settings automatically.
* **Marking and Visual Indicators**:
  + Labels can include visual markings, such as watermarks or headers, to indicate sensitivity.
* **Label Customization**:
  + Customize label visuals to fit organizational branding and requirements.
* **Monitoring and Auditing**:
  + Continuously monitor protection settings and marking to ensure compliance and effectiveness.
* **User Experience**:
  + Educate users on how labels affect content and the importance of following labeling guidelines.
* **Review and Adjustment**:
  + Periodically review and adjust label protection settings and marking as needed to align with evolving data requirements.
* **Documentation**:
  + Maintain documentation of label configurations, protection settings, and visual markings for compliance and auditing purposes.

## Design and implement encryption for email messages

### Design an email encryption solution based on methods available in Microsoft 365

* **Email Encryption**:
  + Email encryption secures the content of email messages to protect sensitive information from unauthorized access.
* **Methods Available in Microsoft 365**:
  + **Office 365 Message Encryption (OME)**:
    - OME allows you to encrypt emails and control access to them.
    - You can set encryption policies based on email content, recipient, or sender.
  + **Sensitivity Labels**:
    - Use sensitivity labels to automatically apply encryption based on content classification.
    - Define label policies that include encryption settings.
  + **Exchange Online Encryption**:
    - Exchange Online supports transport layer security (TLS) for secure email communication.
    - Use Transport Rules to enforce encryption for specific email conditions.
  + **Azure Information Protection (AIP)**:
    - AIP integrates with Microsoft 365 to provide advanced encryption and rights management capabilities.
    - It allows you to classify and protect emails with granular control.
* **Design Considerations**:
  + Identify the sensitivity of email content and data classification requirements.
  + Determine whether encryption should be automatic, manual, or based on specific criteria.
  + Define policies for key management and access controls.
  + Consider user training and awareness for proper encryption usage.
* **Compliance and Legal Requirements**:
  + Ensure the email encryption solution aligns with regulatory compliance (e.g., GDPR, HIPAA).
* **Testing and Validation**:
  + Test the email encryption solution with sample emails to verify proper functioning.
* **Documentation**:
  + Maintain documentation on the email encryption solution design, policies, and configurations.

### Implement Microsoft Purview Message Encryption

1. **Overview:**
   * Standard data encryption feature in Purview.
   * Provides basic encryption for safeguarding data.
2. **Encryption Methods:**
   * Utilizes industry-standard encryption like TLS for data in transit.
   * Azure Storage Service Encryption for data at rest.
3. **Key Management:**
   * Leverages Azure Key Vault for secure key storage and management.
4. **User Experience:**
   * Allows users to send and receive encrypted messages and documents.
   * Decryption is accessible to authorized recipients.
5. **Compliance and Auditing:**
   * Helps meet compliance requirements by providing audit trails and logs.

### Implement Microsoft Purview Advanced Message Encryption

1. **Overview:**
   * Enhanced data protection solution for Purview.
   * Offers more advanced encryption capabilities.
2. **Features:**
   * Extends Purview Message Encryption with additional features.
   * Supports data classification, labeling, and automatic encryption based on policies.
3. **Integration with Azure Information Protection:**
   * Integrates with Azure Information Protection for advanced data classification and labeling.
4. **User Experience:**
   * Provides more comprehensive encryption options for data, including granular control over who can access it.
5. **Compliance and Auditing:**
   * Offers advanced compliance features for tracking and auditing encrypted data.

**Comparison Advance VS Regular:**

* Purview Advanced Message Encryption builds upon the standard Purview Message Encryption, offering more advanced encryption features, especially in terms of data classification and policy-based automatic encryption. It provides a higher level of control and security for sensitive data.

# Implement DLP (15–20%)

## Create and configure DLP policies

### Design DLP policies based on an organization’s requirements

* **DLP Overview:** Data Loss Prevention (DLP) policies safeguard sensitive data within an organization by monitoring and controlling its movement.
* **Steps to Design DLP Policies:**
  1. **Identify Sensitive Data:** Determine what data is sensitive, such as financial records or customer information.
  2. **Compliance Requirements:** Consider industry and regulatory rules (e.g., GDPR, HIPAA) to align policies.
  3. **User Roles:** Define roles and their data access levels, ensuring not all users have the same permissions.
  4. **Policy Types:** Create policies (e.g., blocking, monitoring, encryption) based on identified data and risks.
  5. **Incident Response:** Develop a plan for handling policy violations, including notifications and remediation.
* **Tools and Technologies:**
  1. **Microsoft 365 Security & Compliance Center:** Utilize this platform to configure and manage DLP policies.
* **Policy Elements:**
  1. **Conditions:** Specify triggers like keywords, sensitive patterns, or content types.
  2. **Actions:** Determine what happens when a policy is violated, such as blocking or alerting.
  3. **Locations:** Define where policies apply, like emails, documents, or SharePoint.
* **Testing and Tuning:** Regularly review and adjust policies to adapt to changing data needs and threats.
* **User Training:** Educate users about DLP policies, their responsibilities, and the importance of data protection.
* **Continuous Monitoring:** Continuously monitor policy effectiveness and adjust as necessary to maintain data security.

### Configure permissions for DLP

* **Permission Overview:** In DLP (Data Loss Prevention), configuring permissions is crucial to control who can create, modify, and manage DLP policies and related tasks.
* **Roles and Permissions:**
  1. **Global Administrator:** Has full access to configure and manage DLP policies and settings across the organization.
  2. **DLP Administrator:** Can create and manage DLP policies but may have restricted access to other Microsoft 365 admin functions.
  3. **Custom Roles:** Organizations can create custom roles with specific DLP-related permissions tailored to their needs.
* **Steps to Configure Permissions:**
  1. **Access Microsoft 365 Security & Compliance Center:** Log in with administrative credentials.
  2. **Role Assignment:** Assign roles to users or groups based on their responsibilities.
  3. **DLP Management Role:** Assign the "DLP Administrator" or custom role to individuals who need to manage DLP policies.
  4. **Testing Permissions:** Ensure users with assigned roles can access DLP settings and create/modify policies as needed.
* **Least Privilege Principle:** Follow the principle of least privilege, granting only necessary permissions to minimize security risks.
* **Regular Review:** Periodically review and update permissions to reflect organizational changes and ensure ongoing security.
* **Documentation:** Maintain documentation of role assignments and permissions for auditing and compliance purposes.

### Create and manage DLP policies

* **DLP Policies Overview:** Data Loss Prevention (DLP) policies in Microsoft 365 help protect sensitive information by monitoring and controlling its use and sharing.
* **Steps to Create and Manage DLP Policies:**
  1. **Access Security & Compliance Center:** Log in to the Microsoft 365 Security & Compliance Center.
  2. **Create a New DLP Policy:**
     + Choose "Create a policy."
     + Select a template or create a custom policy based on your organization's needs.
     + Define policy settings, such as conditions (e.g., keywords, content types), actions (e.g., block, notify), and exceptions.
  3. **Policy Testing:** Use policy tips to test the impact of policies on emails and documents.
  4. **Deploy Policies:**
     + Choose the locations where the policy applies (e.g., Exchange, SharePoint, OneDrive).
     + Specify the scope (e.g., all users, specific groups).
  5. **Monitoring and Reporting:**
     + Monitor policy violations and incidents in the DLP dashboard.
     + Review reports and logs to track policy effectiveness and violations.
  6. **Policy Optimization:**
     + Continuously refine and update policies based on insights from monitoring and reporting.
  7. **Exceptions and Overrides:**
     + Define exceptions for specific scenarios where policy enforcement should not apply.
     + Allow authorized users to override policy actions when necessary.
* **User Education:** Train employees on DLP policies, their implications, and responsible data handling.
* **Incident Response:** Develop a plan to respond to policy violations, including notification, investigation, and remediation.

### Interpret policy and rule precedence in DLP

* **Policy Precedence Overview:** In Data Loss Prevention (DLP), policy precedence determines which policy or rule takes precedence when multiple policies potentially apply to the same content.
* **Key Concepts:**
  1. **Rule Priority:** DLP policies consist of rules with different priorities. Lower numerical values indicate higher priority.
  2. **Policy Inheritance:** Policies can be assigned at different levels, such as organization-wide or specific to a site or user group.
  3. **Order of Evaluation:** DLP evaluates policies in a specific order: Built-in, user-defined, and then custom.
* **Precedence Rules:**
  1. **User Overrides:** If a user has the permission to override a policy, their actions take precedence over the policy's enforcement.
  2. **Custom Policies:** Custom policies typically take precedence over built-in policies because they are specific to your organization's needs.
  3. **Policy Scope:** More specific policies (e.g., site-specific) take precedence over broader policies (e.g., organization-wide).
  4. **Rule Priority:** Rules with lower numerical priorities (higher priority) take precedence over rules with higher numerical priorities.
* **Conflict Resolution:**
  1. When conflicts arise between policies or rules, the policy or rule with the highest precedence is enforced.
* **Testing and Validation:** Use policy testing and simulations to understand how policies interact and to ensure the desired behavior.
* **Documentation:** Maintain a clear record of policy hierarchy, scope, and priorities to manage and troubleshoot policy interactions effectively.

### Configure a Microsoft Defender for Cloud Apps file policy to use DLP policies

* **Overview:** Microsoft Defender for Cloud Apps helps secure cloud services like SharePoint, OneDrive, and Teams. You can enhance protection by integrating DLP policies.
* **Steps to Configure File Policy with DLP:**
  1. **Access Microsoft Defender for Cloud Apps Dashboard:** Log in to the Microsoft 365 Defender portal.
  2. **Create a New File Policy:**
     + Click on "File policies."
     + Choose "Create a policy" and provide a name and description.
  3. **Define Conditions:**
     + Specify conditions based on DLP settings (e.g., sensitive information types, content inspection, sharing settings).
  4. **Set Actions:**
     + Determine actions when a violation occurs (e.g., block access, notify admins).
  5. **Enable DLP Integration:**
     + Under "File governance," enable the integration with DLP.
     + Link the DLP policy you want to associate with this file policy.
  6. **Scope and Assign Policy:**
     + Define the scope by selecting target services (e.g., SharePoint, OneDrive).
     + Assign the policy to users, groups, or sites as needed.
  7. **Review and Save:** Double-check policy settings and save the configuration.
* **Testing and Monitoring:**
  1. Use policy simulations and monitoring to ensure the policy functions as intended without causing disruptions.
* **Documentation and Compliance:** Maintain records of policy configurations for auditing and compliance purposes.

## Implement and monitor Endpoint DLP

### Configure advanced DLP rules for devices in DLP policies

* **Overview:** Microsoft Defender for Cloud Apps helps secure cloud services like SharePoint, OneDrive, and Teams. You can enhance protection by integrating DLP policies.
* **Steps to Configure File Policy with DLP:**
  1. **Access Microsoft Defender for Cloud Apps Dashboard:** Log in to the Microsoft 365 Defender portal.
  2. **Create a New File Policy:**
     + Click on "File policies."
     + Choose "Create a policy" and provide a name and description.
  3. **Define Conditions:**
     + Specify conditions based on DLP settings (e.g., sensitive information types, content inspection, sharing settings).
  4. **Set Actions:**
     + Determine actions when a violation occurs (e.g., block access, notify admins).
  5. **Enable DLP Integration:**
     + Under "File governance," enable the integration with DLP.
     + Link the DLP policy you want to associate with this file policy.
  6. **Scope and Assign Policy:**
     + Define the scope by selecting target services (e.g., SharePoint, OneDrive).
     + Assign the policy to users, groups, or sites as needed.
  7. **Review and Save:** Double-check policy settings and save the configuration.
* **Testing and Monitoring:**
  1. Use policy simulations and monitoring to ensure the policy functions as intended without causing disruptions.
* **Documentation and Compliance:** Maintain records of policy configurations for auditing and compliance purposes.

### Configure Endpoint DLP settings

* **Endpoint DLP Overview:** Endpoint Data Loss Prevention (DLP) extends data protection to devices like PCs and mobile devices. Configuring settings is vital for safeguarding sensitive data.
* **Steps to Configure Endpoint DLP Settings:**
  1. **Access Microsoft 365 Security & Compliance Center:**
     + Log in with administrative credentials.
  2. **Enable Endpoint DLP:**
     + Navigate to the Security & Compliance Center.
     + Under "Data loss prevention," choose "Endpoint DLP."
  3. **Create DLP Policies:**
     + Define DLP policies specifying conditions, actions, and sensitive data types.
  4. **Assign Policies:**
     + Assign policies to user groups or devices based on organizational needs.
  5. **Endpoint DLP Settings:**
     + Configure settings like notification preferences, protection rules, and content scan locations.
  6. **Content Scan Locations:**
     + Determine which locations on endpoints to monitor (e.g., documents, emails).
  7. **Protection Rules:**
     + Set rules for actions like blocking, warning, or allowing specific activities.
  8. **Notifications:**
     + Configure notification settings for policy violations (e.g., email alerts to admins).
  9. **Policy Testing:**
     + Use policy tips to simulate policy violations and assess their impact.
  10. **Monitoring and Reporting:**
      + Continuously monitor policy violations using the DLP dashboard and generate reports.
  11. **Incident Response:**
      + Develop a plan for handling policy violations, including investigation and remediation.
* **User Education:** Train end-users on Endpoint DLP policies, their implications, and responsible data handling on their devices.
* **Documentation:** Maintain records of policy configurations and incident responses for auditing and compliance purposes.

### Recommend a deployment method for device onboarding

* **Device Onboarding Overview:** Device onboarding is a critical step in securing and managing devices within an organization's network. The choice of deployment method depends on various factors, including the organization's size, security requirements, and device types.
* **Deployment Methods:**
  1. **Manual Onboarding:**
     + Suitable for small-scale deployments or environments with limited resources.
     + Requires users or IT administrators to manually configure devices with necessary security settings, certificates, and access controls.
     + Provides fine-grained control but can be time-consuming for larger deployments.
  2. **Mobile Device Management (MDM) Solutions:**
     + Ideal for managing mobile devices like smartphones and tablets.
     + Organizations can use MDM platforms like Microsoft Intune to automate onboarding processes.
     + Offers centralized management, over-the-air provisioning, and policy enforcement.
  3. **Mobile Application Management (MAM):**
     + Focused on managing applications and data on mobile devices.
     + MAM solutions allow for secure app distribution and data protection without full device control.
     + Useful when BYOD (Bring Your Own Device) policies are in place.
  4. **Azure Active Directory Join:**
     + Streamlines onboarding for Windows devices, allowing them to join Azure AD directly.
     + Provides seamless access to organizational resources and simplifies authentication and management.
  5. **Network Access Control (NAC):**
     + Controls device onboarding by checking device health and compliance before granting network access.
     + Ensures that only compliant devices can connect to the network.
* **Recommendation Considerations:**
  1. **Organization Size:** Large organizations may benefit from automated solutions like MDM or Azure AD Join to scale onboarding efficiently.
  2. **Device Types:** Consider the types of devices (e.g., mobile, desktop) and their operating systems when choosing a method.
  3. **Security Requirements:** Evaluate the organization's security needs, including data protection and access control.
  4. **User Experience:** Balance security with user convenience to ensure a smooth onboarding process.
* **Documentation:** Maintain clear documentation of the chosen deployment method and onboarding processes for reference and auditing.

### Identify endpoint requirements for device onboarding

* **Endpoint Requirements Overview:** Ensuring that endpoints (devices) meet specific criteria is crucial for successful and secure device onboarding. These requirements help maintain a standardized and secure computing environment.
* **Common Endpoint Requirements:**
  1. **Device Type:** Determine the type of device being onboarded, such as desktops, laptops, smartphones, or tablets.
  2. **Operating System:** Identify the device's operating system (e.g., Windows, macOS, iOS, Android) and its version.
  3. **Patch Levels:** Verify that the device has the latest operating system updates and security patches installed to address vulnerabilities.
  4. **Hardware Specifications:** Check if the device meets minimum hardware requirements for performance and compatibility.
  5. **Security Software:** Ensure that essential security software, such as antivirus, anti-malware, and firewalls, is installed and up to date.
  6. **Encryption:** Evaluate if the device uses encryption to protect data at rest (disk encryption) and data in transit (network encryption).
  7. **Authentication Mechanisms:** Confirm the use of strong authentication methods, including passwords, PINs, biometrics, or multi-factor authentication (MFA).
  8. **Compliance with Policies:** Ensure that the device complies with organizational security policies and configuration standards.
  9. **Software and Application Whitelisting:** Implement a list of approved software and applications to prevent unauthorized installations.
  10. **Mobile Device Management (MDM) Enrollment:** For mobile devices, verify that the device is enrolled in an MDM solution for management and policy enforcement.
  11. **Network Connectivity:** Ensure that the device has access to a secure network, such as a corporate VPN, if required.
* **Documentation:** Maintain records of endpoint requirements, compliance checks, and any remediation actions taken.
* **Automated Tools:** Consider using endpoint management and security tools to automate compliance checks and enforce policies.
* **Onboarding Workflow:** Integrate endpoint requirements into the device onboarding process to ensure that devices meet criteria before granting access to network resources.

### Monitor endpoint activities

* **Endpoint Activity Monitoring Overview:**
  + Monitoring endpoint activities is crucial for identifying security threats, ensuring compliance, and maintaining the overall health of devices within an organization.
* **Key Aspects of Monitoring:**
  + **Endpoint Visibility:**
    - Gain visibility into all endpoints connected to the network, including PCs, laptops, mobile devices, and servers.
  + **Real-Time Monitoring:**
    - Continuously monitor endpoint activities in real-time to detect and respond to security incidents promptly.
  + **Logging and Auditing:**
    - Enable logging and auditing on endpoints to record events and activities for later analysis.
  + **Alerting and Notifications:**
    - Set up alerts and notifications for unusual or suspicious activities to enable rapid incident response.
  + **Compliance Monitoring:**
    - Ensure that endpoints adhere to security and compliance policies, such as patch management and access controls.
  + **User and Device Behavior Analysis:**
    - Analyze user and device behavior patterns to detect anomalies and potential security threats.
  + **Threat Detection:**
    - Implement threat detection mechanisms to identify malware, intrusions, and other security risks.
  + **Data Loss Prevention (DLP):**
    - Monitor data movement on endpoints to prevent data leaks and ensure sensitive data protection.
  + **Endpoint Security Solutions:**
    - Utilize endpoint security solutions, such as antivirus, anti-malware, and EDR (Endpoint Detection and Response), for comprehensive protection.
  + **Incident Response:**
    - Develop an incident response plan to address security incidents promptly and effectively.
* **Logging and Monitoring Tools:**
  + Employ logging and monitoring tools like Microsoft Defender for Endpoint, SIEM (Security Information and Event Management) systems, and EDR solutions.
* **Continuous Improvement:**
  + Regularly review and refine monitoring strategies to adapt to evolving threats and vulnerabilities.
* **Documentation:**
  + Maintain comprehensive records of endpoint activities, incidents, and response actions for auditing and compliance purposes.

### Implement the Microsoft Purview Extension

* **Overview of Microsoft Purview Extension:**
  + Microsoft Purview is a data governance solution that helps organizations discover, catalog, and manage their data assets. The Purview Extension enables integration with other data sources and systems.
* **Key Steps to Implement the Purview Extension:**
  + **Access Purview Portal:**
    - Log in to the Microsoft Purview portal with appropriate administrative credentials.
  + **Navigate to Extensions:**
    - Within the Purview portal, find and access the Extensions section or menu.
  + **Install or Configure Extension:**
    - Depending on your specific integration needs, either install an existing extension or configure a custom extension.
  + **Select Data Source or System:**
    - Choose the data source or system you want to integrate with Purview. This could be a database, data lake, or other data repositories.
  + **Provide Connection Details:**
    - Enter the necessary connection details, such as server addresses, credentials, and authentication methods.
  + **Define Data Cataloging and Discovery Settings:**
    - Configure how the extension should catalog and discover data assets from the connected source. This may involve defining data classifications, metadata, and data lineage.
  + **Schedule Data Scans (if applicable):**
    - Set up scheduled scans to ensure that Purview stays up to date with changes in the integrated data source.
  + **Test the Integration:**
    - Before deploying the extension in a production environment, thoroughly test the integration to ensure it works as expected.
  + **Documentation:**
    - Maintain documentation of the extension configuration, including connection details, settings, and any custom configurations.
* **Monitoring and Maintenance:**
  + Continuously monitor the extension's performance and data discovery. Address any issues promptly and update configurations as needed.
* **Security Considerations:**
  + Ensure that security best practices are followed when integrating with external data sources to protect sensitive information.

## Monitor and manage DLP activities

### Analyze DLP reports

* **DLP Reports Overview:**
  + Data Loss Prevention (DLP) reports provide valuable insights into an organization's data protection efforts. Analyzing these reports is crucial for maintaining data security and compliance.
* **Key Aspects of Analyzing DLP Reports:**
  + **Accessing Reports:**
    - Log in to the DLP management console or the Microsoft 365 Security & Compliance Center to access DLP reports.
  + **Report Types:**
    - Understand the different types of DLP reports available, including policy violation reports, incident reports, and activity reports.
  + **Filtering and Customization:**
    - Use filters and customization options to narrow down the data and focus on specific aspects of interest.
  + **Incident Analysis:**
    - Review incident reports to identify data breaches, policy violations, or suspicious activities.
  + **Policy Effectiveness:**
    - Evaluate policy violation reports to assess the effectiveness of DLP policies and identify areas for improvement.
  + **Data Trends:**
    - Analyze activity reports to identify data usage trends, patterns, and potential risks.
  + **User and Device Insights:**
    - Gain insights into user and device behavior by examining user-centric and device-centric reports.
  + **Export and Sharing:**
    - Export reports for further analysis, share findings with relevant stakeholders, and use reports for compliance audits.
  + **Incident Resolution:**
    - Use DLP reports to investigate incidents and take appropriate remediation actions.
  + **Continuous Improvement:**
    - Use insights from DLP reports to refine DLP policies, user training, and security practices.
* **Compliance Auditing:**
  + DLP reports are valuable for demonstrating compliance with data protection regulations, such as GDPR or HIPAA.
* **Documentation:**
  + Maintain records of DLP reports and actions taken based on report findings for compliance and auditing purposes.

### Analyze DLP activities by using Activity explorer

* **Activity Explorer Overview:**
  + Activity Explorer is a feature in Microsoft's Data Loss Prevention (DLP) solution that provides detailed insights into data-related activities within an organization's Microsoft 365 environment.
* **Key Steps to Analyze DLP Activities with Activity Explorer:**
  + **Access Activity Explorer:**
    - Log in to the Microsoft 365 Security & Compliance Center with administrative credentials.
  + **Navigate to DLP Dashboard:**
    - From the Security & Compliance Center, go to the DLP dashboard.
  + **Access Activity Explorer:**
    - Within the DLP dashboard, select "Activity explorer" or a similar option.
  + **Choose Filters and Time Frame:**
    - Apply filters to specify the data you want to analyze, such as date ranges, users, or specific DLP policies.
  + **View Activity Data:**
    - Activity Explorer presents a visual representation of data activities, including email communication, document sharing, and more.
  + **Use Graphs and Charts:**
    - Utilize graphs, charts, and visual representations to understand data movement patterns and trends.
  + **Drill Down for Details:**
    - Click on specific data points to access more detailed information about activities, users, and data sources.
  + **Filter by Policy Violations:**
    - Focus on activities that resulted in policy violations or potential data leaks.
  + **Investigate Anomalies:**
    - Identify unusual or suspicious activities and investigate further to determine if they pose security risks.
  + **Generate Reports:**
    - Generate reports from Activity Explorer for documentation, compliance, and auditing purposes.
* **Incident Response:**
  + Activity Explorer can aid in incident response by providing a clear view of data activities leading up to and during an incident.
* **Policy Optimization:**
  + Use insights from Activity Explorer to refine and optimize DLP policies based on observed data behavior.
* **Documentation:**
  + Maintain records of activity analysis, findings, and actions taken for future reference and auditing.

### Remediate DLP alerts in the Microsoft Purview compliance portal

* **DLP Alert Remediation Overview:**
  + Remediation involves taking action to address and resolve Data Loss Prevention (DLP) alerts and policy violations within the Microsoft Purview Compliance Portal.
* **Key Steps to Remediate DLP Alerts:**
  + **Access the Purview Compliance Portal:**
    - Log in to the Microsoft Purview Compliance Portal using appropriate administrative credentials.
  + **Navigate to DLP Alerts:**
    - Within the portal, locate and access the section or menu dedicated to DLP alerts and incidents.
  + **Review Alert Details:**
    - Select the specific DLP alert you want to remediate and review the alert details for context.
  + **Assess Severity and Impact:**
    - Evaluate the severity and potential impact of the alert to prioritize remediation efforts.
  + **Identify Affected Data and Users:**
    - Determine which data or users are affected by the policy violation indicated in the alert.
  + **Take Remediation Actions:**
    - Based on the nature of the alert, take appropriate actions to remediate the issue. Common actions include:
      * Removing sensitive data from unauthorized locations.
      * Blocking data sharing or downloads.
      * Notifying the user or administrator about the violation.
      * Initiating an incident response process for severe breaches.
  + **Document Remediation Actions:**
    - Maintain records of the actions taken to address the DLP alert, including timestamps and details.
  + **Resolve Alert:**
    - Mark the alert as resolved or closed in the Purview Compliance Portal once remediation is complete.
  + **Continuous Monitoring:**
    - Continue monitoring DLP alerts to ensure that the remediation actions are effective and that similar incidents are prevented in the future.
  + **Policy Optimization:**
    - Use insights from resolved alerts to refine and optimize DLP policies to reduce future violations.
* **Incident Response Planning:**
  + Establish and follow incident response plans for severe DLP alerts that may indicate data breaches.
* **Compliance and Reporting:**
  + Maintain documentation of DLP alerts, remediation actions, and resolutions for compliance and auditing purposes.

### Remediate DLP alerts generated by Defender for Cloud Apps

* **DLP Alert Remediation Overview:**
  + Remediation involves taking action to address and resolve Data Loss Prevention (DLP) alerts generated by Microsoft Defender for Cloud Apps to protect sensitive data.
* **Key Steps to Remediate DLP Alerts:**
  + **Access Microsoft Defender for Cloud Apps Dashboard:**
    - Log in to the Microsoft 365 Defender portal or the relevant security console with administrative credentials.
  + **Navigate to DLP Alerts:**
    - Find and access the section or menu dedicated to DLP alerts and incidents within Defender for Cloud Apps.
  + **Review Alert Details:**
    - Select the specific DLP alert you want to remediate and review the alert details for context.
  + **Assess Severity and Impact:**
    - Evaluate the severity and potential impact of the alert to prioritize remediation efforts.
  + **Identify Affected Data and Users:**
    - Determine which data or users are affected by the policy violation indicated in the alert.
  + **Take Remediation Actions:**
    - Based on the nature of the alert, take appropriate actions to remediate the issue. Common actions include:
      * Removing or restricting access to sensitive data.
      * Blocking data sharing or downloads.
      * Notifying the user or administrator about the violation.
      * Initiating an incident response process for severe breaches.
  + **Document Remediation Actions:**
    - Maintain records of the actions taken to address the DLP alert, including timestamps and details.
  + **Resolve Alert:**
    - Mark the alert as resolved or closed within the Defender for Cloud Apps console once remediation is complete.
  + **Continuous Monitoring:**
    - Continue monitoring DLP alerts to ensure that the remediation actions are effective and that similar incidents are prevented in the future.
  + **Policy Optimization:**
    - Use insights from resolved alerts to refine and optimize DLP policies to reduce future violations.
* **Incident Response Planning:**
  + Establish and follow incident response plans for severe DLP alerts that may indicate data breaches.
* **Compliance and Reporting:**
  + Maintain documentation of DLP alerts, remediation actions, and resolutions for compliance and auditing purposes.

# Implement data lifecycle and records management (10–15%)

## Retain and delete data by using retention labels

### Plan for information retention and disposition by using retention labels

1. **Retention Labels Overview**:
   * Retention labels are used to classify content and define how long it should be retained and what actions should be taken when the retention period expires.
2. **Creating Retention Labels**:
   * Use the Microsoft 365 Compliance Center or Security & Compliance Center to create retention labels.
   * Specify a name, description, retention period, and actions (delete, archive, or do nothing).
3. **Assigning Labels**:
   * Apply labels to content manually, automatically (based on conditions), or through default policies.
4. **Information Governance**:
   * Retention labels are a critical part of an organization's information governance strategy.
   * They help ensure compliance with legal and regulatory requirements.
5. **Retention Actions**:
   * Configure actions like deletion, archival, or nothing when a retention label's duration is met.
   * Use actions to align with data retention policies.
6. **Custom Labels vs. Default Labels**:
   * Custom labels are created for specific content, while default labels apply broadly.
   * Default labels can be set as organization-wide policies.
7. **Retention Labels and Sensitivity Labels**:
   * Retention labels can be used in conjunction with sensitivity labels to classify and protect sensitive information.
8. **Monitoring and Reporting**:
   * Regularly review and audit retention labels and their application.
   * Utilize compliance reports and logs for insights into data retention compliance.
9. **User Training and Communication**:
   * Educate users about retention labels and their importance.
   * Ensure employees understand their role in data retention and disposition.
10. **Review and Adjust**:
    * Periodically review and adjust retention label policies as business needs and regulations change.

### Create retention labels for data lifecycle management

1. **Access Compliance Center**: Sign in to Microsoft 365 Compliance Center.
2. **Navigate to Labels**: Go to "Information governance" and select "Retention."
3. **Create a Label**:
   * Click "Create a label."
   * Give it a name and description.
   * Choose whether it's a retention or deletion label.
   * Define retention settings:
     + Retention duration.
     + Actions (delete, move, or retain).
     + Locations (where it applies).
4. **Advanced Settings**:
   * Decide if it should apply to all items or only specific content.
   * Enable event-based retention triggers if needed.
5. **Review & Save**: Review your settings and save the label.
6. **Publish Label**: Publish it to make it available for users.
7. **Apply Labels**:
   * Assign labels to content manually or automatically.
   * Use auto-labeling policies if required.
8. **Monitor & Review**: Regularly review label effectiveness and make adjustments as necessary.
9. **Test and Train**: Test your label policies in a controlled environment and train users on label usage.
10. **Compliance Review**: Ensure compliance with legal and regulatory requirements.

### Configure and manage adaptive scopes

1. **Access Microsoft 365 Security Center**:
   * Sign in to the Microsoft 365 Security Center.
2. **Navigate to Adaptive Scopes**:
   * Click on "Settings" in the left menu.
   * Under "Advanced features," select "Adaptive scopes."
3. **Create Adaptive Scopes**:
   * Click "Create" to define a new adaptive scope.
   * Name the scope and provide a description for clarity.
4. **Configure Scope Criteria**:
   * Define the criteria that determine which resources are included in the scope.
   * Use filters such as location, sensitivity labels, or other attributes.
5. **Review and Save**:
   * Review the scope settings for accuracy.
   * Save the scope once all criteria are set.
6. **Apply Adaptive Scopes**:
   * Assign adaptive scopes to relevant security policies or rules.
   * Scopes can be applied to Threat protection policies, Data loss prevention (DLP) policies, etc.
7. **Monitor and Fine-Tune**:
   * Continuously monitor the effectiveness of adaptive scopes.
   * Adjust scope criteria as needed to align with security objectives.
8. **Documentation and Training**:
   * Document the adaptive scope configurations for reference.
   * Train relevant personnel on the use and management of adaptive scopes.
9. **Compliance and Reporting**:
   * Regularly assess compliance with adaptive scope policies.
   * Generate reports to track the impact of the scopes on security measures.
10. **Review and Update**:
    * Periodically review and update adaptive scopes to adapt to changing security requirements or resource configurations.

### Configure a retention label policy to publish labels

1. **Access Compliance Center**:
   * Sign in to Microsoft 365 Compliance Center.
2. **Navigate to Retention Label Policies**:
   * Go to "Information governance" and select "Retention."
3. **Create or Edit Policy**:
   * Choose an existing policy or create a new one.
4. **Add a Label**:
   * Within the policy settings, add a retention label.
5. **Configure Label Settings**:
   * Define retention settings for the label:
     + Retention duration.
     + Actions (delete, move, or retain).
     + Locations (where it applies).
6. **Publish Labels**:
   * Ensure the "Publish this label to users" option is selected.
   * Choose whether to allow users to classify content.
7. **Advanced Settings**:
   * Configure advanced options if needed, like event-based retention.
8. **Scope and Review**:
   * Define the scope of the policy (e.g., specific users or locations).
   * Review and save the policy.
9. **Assign Policy**:
   * Assign the policy to relevant users or groups.
10. **Test and Monitor**:
    * Test the policy in a controlled environment.
    * Monitor label application and user feedback.
11. **Document and Train**:
    * Document policy details and procedures.
    * Train users on label usage and policy implications.
12. **Compliance Review**:
    * Ensure compliance with legal and regulatory requirements.
    * Regularly review and update the policy as needed.

### Configure a retention label policy to auto-apply labels

1. **Access Compliance Center**:
   * Sign in to Microsoft 365 Compliance Center.
2. **Navigate to Retention Label Policies**:
   * Go to "Information governance" and select "Retention."
3. **Create or Edit Policy**:
   * Choose an existing policy or create a new one.
4. **Add a Label**:
   * Within the policy settings, add a retention label.
5. **Configure Label Settings**:
   * Define retention settings for the label:
     + Retention duration.
     + Actions (delete, move, or retain).
     + Locations (where it applies).
6. **Auto-Apply Settings**:
   * Enable the "Auto-apply this label" option.
7. **Define Conditions**:
   * Specify conditions for label auto-application:
     + Choose criteria like content type, keywords, or sensitivity labels.
8. **Scope and Review**:
   * Define the scope of the policy (e.g., specific users or locations).
   * Review and save the policy.
9. **Assign Policy**:
   * Assign the policy to relevant users or groups.
10. **Test and Monitor**:
    * Test the policy in a controlled environment.
    * Monitor label auto-application and adjust conditions as needed.
11. **Document and Train**:
    * Document policy details and procedures.
    * Train users on label auto-application and its implications.
12. **Compliance Review**:
    * Ensure compliance with legal and regulatory requirements.
    * Regularly review and update the policy as needed.

### Interpret the results of policy precedence, including using Policy lookup

1. **Policy Precedence Basics**:
   * Understand that multiple policies can apply to Microsoft 365 services.
   * Policies are evaluated in a specific order, and the policy with the highest precedence takes effect.
2. **Policy Types**:
   * Be familiar with different policy types, such as Conditional Access policies, Retention policies, and Sensitivity Label policies.
3. **Policy Evaluation Order**:
   * Policies are evaluated in this order:
     + Global policies
     + Service-specific policies
     + User or group policies
4. **Policy Conflicts**:
   * Know that conflicts can arise when multiple policies overlap.
   * Conflicts can result in unexpected behavior.
5. **Policy Lookup**:
   * Use "Policy lookup" to analyze policy precedence:
     + In the Microsoft 365 Compliance Center, go to "Information governance" > "Policy lookup."
     + Enter relevant information like users, groups, and services.
     + Review the list of policies that apply and their precedence.
6. **Evaluate Policy Results**:
   * Policies with higher precedence override those with lower precedence.
   * Carefully review the policy lookup results to understand which policies are in effect for a specific scenario.
7. **Resolve Conflicts**:
   * If conflicts exist, resolve them by adjusting policy settings, priorities, or scoping.
8. **Test and Verify**:
   * After making changes, thoroughly test policies to ensure they behave as expected.
9. **Documentation and Reporting**:
   * Keep detailed records of policy configurations and their precedence.
   * Generate reports to document and audit policy effects.
10. **Stay Informed**:
    * Stay updated on Microsoft 365 policy changes and best practices to maintain effective policy management.

## Manage data retention in Microsoft 365 workloads

### Create and apply retention policies for SharePoint and OneDrive

1. **Retention Policies Overview**:
   * DLP Retention policies control how long content should be retained and what actions to take when the retention period ends.
2. **Creating Retention Policies**:
   * Use the Microsoft 365 Compliance Center or SharePoint admin center.
   * Specify a name, duration, and actions (delete, archive, or nothing).
3. **Applying Retention Policies**:
   * Assign policies to SharePoint sites, OneDrive accounts, or individual documents and folders.
4. **Default Retention Labels**:
   * SharePoint and OneDrive may have default retention labels that align with compliance standards.
5. **Customizing Policies**:
   * Customize policies based on organizational needs, legal requirements, or specific content types.
6. **Automatic Application**:
   * Policies can be applied automatically based on content types, metadata, or keywords.
7. **Coexistence with Retention Labels**:
   * Retention policies can coexist with retention labels, offering granular control.
8. **Communication and Training**:
   * Educate users about retention policies and how they impact their SharePoint and OneDrive data.
9. **Monitoring and Reporting**:
   * Regularly review compliance reports to ensure policies are being enforced correctly.
10. **Adjusting Policies**:
    * Periodically assess and adjust retention policies to align with changing business requirements and regulations.

### Create and apply retention policies for Microsoft 365 groups

1. **Retention Policies for Microsoft 365 Groups**:
   * DLP Retention policies help control how long data within Microsoft 365 Groups is retained and what actions should be taken when retention periods end.
2. **Creating Retention Policies**:
   * Use the Microsoft 365 Compliance Center or PowerShell to create retention policies for Groups.
   * Specify the policy name, duration, and actions (delete, archive, or nothing).
3. **Assigning Policies to Groups**:
   * Apply retention policies to Microsoft 365 Groups to manage their data.
   * Policies can be assigned at the organization-wide level or for specific Groups.
4. **Default Retention Policies**:
   * Default retention policies may be available, aligning with common compliance requirements.
5. **Customizing Policies**:
   * Customize retention policies to meet specific organizational needs, legal obligations, or content types.
6. **Automatic Application**:
   * Policies can be automatically applied based on content types, keywords, or metadata.
7. **Communication and Training**:
   * Educate users about retention policies for Microsoft 365 Groups and how they impact data within the Groups.
8. **Monitoring and Reporting**:
   * Regularly review compliance reports to ensure policies are effectively enforced.
9. **Policy Adjustments**:
   * Periodically assess and adjust retention policies to align with evolving business requirements and regulations.

### Create and apply retention policies for Teams

1. **Retention Policies for Microsoft Teams**:
   * Retention policies help control how long data within Microsoft Teams is retained and what actions should be taken when retention periods end.
2. **Creating Retention Policies**:
   * Use the Microsoft 365 Compliance Center or PowerShell to create retention policies for Teams.
   * Specify policy name, duration, and actions (delete, archive, or nothing).
3. **Assigning Policies to Teams**:
   * Apply retention policies to Microsoft Teams to manage their data.
   * Policies can be assigned at the organization-wide level or for specific Teams.
4. **Default Retention Policies**:
   * Default retention policies may be available to align with common compliance requirements.
5. **Customizing Policies**:
   * Customize retention policies to meet specific organizational needs, legal obligations, or content types.
6. **Automatic Application**:
   * Policies can be automatically applied based on content types, keywords, or metadata.
7. **Communication and Training**:
   * Educate users about retention policies for Microsoft Teams and how they impact data within Teams.
8. **Monitoring and Reporting**:
   * Regularly review compliance reports to ensure policies are effectively enforced.
9. **Policy Adjustments**:
   * Periodically assess and adjust retention policies to align with evolving business requirements and regulations.

### Create and apply retention policies for Yammer

1. **Yammer Retention Policies Overview**:
   * Retention policies in Yammer control how long data is retained and what actions should be taken when retention periods expire.
2. **Creating Yammer Retention Policies**:
   * Use the Microsoft 365 Compliance Center or PowerShell to create retention policies for Yammer.
   * Specify policy name, duration, and actions (delete, archive, or nothing).
3. **Assigning Policies to Yammer**:
   * Apply retention policies to specific Yammer groups or organization-wide.
   * Policies can target messages, files, and other Yammer content.
4. **Default Retention Policies**:
   * Default retention policies may be available in Yammer to align with common compliance requirements.
5. **Customization of Policies**:
   * Customize retention policies to meet specific organizational needs, legal obligations, or content types.
6. **Automatic Policy Application**:
   * Policies can be automatically applied based on content types, keywords, or metadata.
7. **User Communication and Training**:
   * Educate users about Yammer retention policies and how they impact data within the platform.
8. **Monitoring and Reporting**:
   * Regularly review compliance reports to ensure policies are correctly enforced in Yammer.
9. **Policy Adjustments**:
   * Periodically assess and adjust Yammer retention policies to align with evolving business requirements and regulations.

### Create and apply retention policies for Exchange Online

1. **Retention Policies Overview**:
   * Retention policies define how long email and data in Exchange Online should be retained and what actions to take when retention periods expire.
2. **Creating Retention Policies**:
   * Use the Microsoft 365 Compliance Center or PowerShell to create retention policies.
   * Specify a policy name, retention duration, and actions (delete, archive, or nothing).
3. **Assigning Policies to Mailboxes**:
   * Apply retention policies to specific mailboxes, groups, or organization-wide.
   * Policies can target email, calendar items, and other mailbox content.
4. **Default Retention Policies**:
   * Default retention policies may be available, aligning with common compliance standards.
5. **Customizing Policies**:
   * Customize retention policies to meet specific organizational needs, legal requirements, or content types.
6. **Automatic Policy Application**:
   * Policies can be automatically applied based on content types, keywords, or metadata.
7. **User Communication and Training**:
   * Educate users about retention policies and their impact on email and mailbox items.
8. **Monitoring and Reporting**:
   * Regularly review compliance reports to ensure policies are effectively enforced in Exchange Online.
9. **Policy Adjustments**:
   * Periodically assess and adjust retention policies to align with changing business needs and regulations.

### Apply mailbox holds in Exchange Online

1. **Mailbox Holds Overview**:
   * Mailbox holds in Exchange Online are used to preserve mailbox items for legal, regulatory, or compliance reasons.
2. **Types of Holds**:
   * **Litigation Hold**: Preserves all mailbox items indefinitely and can be applied to specific mailboxes.
   * **In-Place Hold**: Preserves mailbox items based on search criteria, including keywords and date ranges.
3. **Applying Holds**:
   * Use the Microsoft 365 Compliance Center or PowerShell to apply mailbox holds.
   * Assign holds to specific mailboxes or mailbox databases.
4. **Preservation Settings**:
   * Configure hold settings, such as retention policies and item holds (e.g., including or excluding specific folders).
5. **Search and Query**:
   * Perform advanced searches to identify and preserve relevant mailbox items.
   * Use the Content Search tool to create and manage searches.
6. **Hold Reports and Auditing**:
   * Regularly review and audit hold reports to ensure compliance with data preservation requirements.
7. **Release and Removal**:
   * When legal requirements are met, release or remove holds to allow for normal mailbox management.
8. **User Education**:
   * Educate users about mailbox holds, their purpose, and how they affect mailbox access and data preservation.

### Implement Exchange Online archiving policies

1. **Archiving Policies Overview**:
   * Archiving policies in Exchange Online help manage mailbox data by automatically moving older items to archive mailboxes.
2. **Archive Mailboxes**:
   * Archive mailboxes are secondary mailboxes associated with a user's primary mailbox for storing historical emails.
3. **Creating Archiving Policies**:
   * Use the Microsoft 365 admin center or PowerShell to create archiving policies.
   * Specify policy settings, including the age at which items should be moved to the archive.
4. **Assigning Policies**:
   * Assign archiving policies to individual users or groups based on their data retention needs.
5. **Default Archive Policy**:
   * Exchange Online may have a default archive policy in place, which can be customized or applied as needed.
6. **Automatic Archiving**:
   * Archiving policies automatically move items to the archive mailbox based on age or other criteria.
7. **User Access to Archives**:
   * Users can access their archive mailbox through Outlook or other mail clients, making it easy to retrieve archived items.
8. **Monitoring and Reporting**:
   * Regularly monitor mailbox sizes and archive usage to ensure policies are effectively managing data.
9. **Adjusting Policies**:
   * Periodically assess and adjust archiving policies to align with evolving business requirements and user needs.

### Configure preservation locks for retention policies and retention label policies

1. **Preservation Locks Overview**:
   * Preservation locks are security controls in Microsoft 365 Compliance Center that prevent the modification or deletion of retention policies and label policies.
2. **Purpose**:
   * Preservation locks ensure that critical retention policies, which govern data retention and deletion, remain intact and compliant.
3. **Levels of Preservation Locks**:
   * There are two levels: Immutable and Locked.
   * Immutable: Prevents any changes to the policy, including deletion. Requires a legal hold to modify.
   * Locked: Allows modification but not deletion. Suitable for scenarios where changes might be necessary but should be restricted.
4. **Applying Preservation Locks**:
   * Use the Microsoft 365 Compliance Center or PowerShell to apply preservation locks to retention policies and label policies.
5. **Retaining Critical Data**:
   * Preservation locks are especially important for ensuring the integrity of policies governing the retention of critical data for compliance and legal purposes.
6. **Lock Duration**:
   * Preservation locks can be set for specific durations or indefinitely, depending on organizational requirements.
7. **Administrator Responsibilities**:
   * Administrators need to carefully manage preservation locks and ensure that they are appropriately configured to meet compliance and legal needs.
8. **Education and Training**:
   * Educate relevant personnel about the importance of preservation locks and the procedures for applying and managing them.

### Recover retained content in Microsoft 365

1. **Retained Content Overview**:
   * Retained content is data that is preserved by retention policies or holds in Microsoft 365.
2. **Recovery Scenarios**:
   * Retained content may need to be recovered for legal eDiscovery, compliance audits, or data loss scenarios.
3. **Methods for Recovery**:
   * Content can be recovered from various locations, including backups, the Recoverable Items folder, or the Preservation Hold Library.
4. **Recoverable Items Folder**:
   * Deleted items, including those under retention, are initially moved to the Recoverable Items folder in Exchange Online.
5. **eDiscovery and Content Search**:
   * Use the Content Search tool in the Microsoft 365 Compliance Center to search for and recover retained content based on criteria like keywords or dates.
6. **Litigation Hold and In-Place Hold**:
   * Mailbox items placed on litigation hold or in-place hold are preserved and can be accessed for recovery purposes.
7. **Preservation Hold Library**:
   * For SharePoint and OneDrive, content preserved due to retention policies is stored in the Preservation Hold Library, allowing for recovery.
8. **Backup Solutions**:
   * Organizations may implement third-party backup solutions for additional data recovery capabilities, but these are separate from native Microsoft 365 features.
9. **Legal and Compliance Considerations**:
   * Follow legal and compliance protocols when recovering retained content, as it may be subject to legal holds or other requirements.
10. **User Education**:
    * Train users and administrators on the proper procedures for recovering retained content to avoid data loss.

## Implement Microsoft Purview records management

### Create and configure retention labels for records management

1. **Retention Labels Overview**:
   * Retention labels are used to classify and manage records, ensuring they are retained or disposed of according to organizational policies.
2. **Creating Retention Labels**:
   * Use the Microsoft 365 Compliance Center or PowerShell to create retention labels.
   * Specify a label name, description, retention duration, and actions (e.g., delete, retain).
3. **Classification and Labeling**:
   * Apply retention labels to documents, emails, and other content to classify them as records.
4. **Default Labels**:
   * Microsoft 365 may offer default retention labels, but custom labels are typically created for specific records management needs.
5. **Retention Actions**:
   * Configure actions like deletion, archival, or nothing for records based on their retention label.
6. **Event-Based Retention**:
   * Use event-based retention triggers to automatically apply labels when specific events occur (e.g., contract expiration).
7. **Disposition Review**:
   * Establish processes for periodic disposition reviews to ensure records are disposed of appropriately or retained as needed.
8. **Label Publishing**:
   * Publish labels to specific locations (e.g., SharePoint libraries) to make them available for content classification.
9. **User Training and Communication**:
   * Educate users about retention labels and their importance in records management.
10. **Monitoring and Reporting**:
    * Regularly monitor compliance with retention labels and generate reports to verify records management adherence.
11. **Legal and Compliance Considerations**:
    * Align retention labels with legal and regulatory requirements for records retention and disposal.
12. **Adjusting and Updating Labels**:
    * Periodically review and update retention labels to reflect changing business needs and compliance standards.

### Manage retention labels by using a file plan, including file plan descriptors

1. **Retention Labels in a File Plan**:
   * A file plan is a structured framework for organizing and managing documents and records, including retention labels.
2. **File Plan Descriptors**:
   * Descriptors are metadata elements that describe aspects of a document or record, such as its purpose, location, or retention requirements.
3. **Creating a File Plan**:
   * Use the Microsoft 365 Compliance Center to create a file plan that outlines the categories, folders, and descriptors for organizing content.
4. **Linking Retention Labels**:
   * Associate retention labels with file plan categories or folders to ensure proper retention and disposition.
5. **Descriptive Metadata**:
   * Assign descriptors to documents and records to provide context and facilitate efficient retrieval and management.
6. **Retention and Disposition Rules**:
   * Define rules within the file plan to specify how long content should be retained and when it should be disposed of based on the associated retention labels.
7. **Applying File Plan Descriptors**:
   * Educate users on the importance of adding accurate descriptors to documents and records when they are created or updated.
8. **Compliance Auditing**:
   * Regularly audit the file plan to ensure that retention labels and descriptors align with current business and compliance needs.
9. **User Training**:
   * Train users on the file plan structure, descriptors, and how they relate to retention labels to encourage consistent use.
10. **File Plan Governance**:
    * Establish governance policies to maintain the integrity of the file plan and its alignment with retention label policies.

### Classify records by using retention labels and retention label policies

1. **Retention Labels for Records Classification**:
   * Retention labels are used to categorize and classify records within Microsoft 365 based on their importance and retention requirements.
2. **Creating Retention Labels**:
   * Use the Microsoft 365 Compliance Center or PowerShell to create retention labels.
   * Specify label names, descriptions, retention durations, and actions (e.g., delete, retain).
3. **Retention Label Policies**:
   * Retention label policies define where and how retention labels should be applied to content, such as SharePoint sites, OneDrive accounts, or email.
4. **Applying Retention Labels**:
   * Assign retention labels manually, automatically based on conditions, or via default policies.
5. **Records Identification**:
   * Retention labels help identify records among vast amounts of data, ensuring they are treated appropriately.
6. **Retention Actions**:
   * Configure actions, like deletion or archival, for records based on their associated retention labels.
7. **Default Retention Labels**:
   * Microsoft 365 may provide default labels that align with common compliance standards.
8. **Automatic Labeling**:
   * Implement auto-labeling policies to apply retention labels automatically based on content characteristics, keywords, or metadata.
9. **User Training and Communication**:
   * Educate users about retention labels, their significance, and how to correctly apply them to records.
10. **Monitoring and Reporting**:
    * Regularly review compliance reports to ensure that retention labels and policies are correctly enforced.
11. **Policy Adjustments**:
    * Periodically assess and adjust retention label policies to meet changing business requirements and compliance regulations.

### Manage event-based retention

1. **Event-Based Retention Overview**:
   * Event-based retention in Microsoft 365 automatically applies retention labels to content based on specific events or triggers.
2. **Use Cases**:
   * Employ event-based retention for scenarios like contract expiration, project completion, or legal holds.
3. **Configuration**:
   * Create event-based retention policies using the Microsoft 365 Compliance Center or PowerShell.
4. **Event Triggers**:
   * Define triggers such as date-based events (e.g., contract end date) or activity-based events (e.g., document finalization).
5. **Retention Actions**:
   * Specify retention actions like deletion, archival, or nothing to occur when the event-based retention trigger is met.
6. **Content Scanning**:
   * Use content searches or automated scanning to identify content that meets event-based retention criteria.
7. **Automation**:
   * Event-based retention policies automate the application of retention labels, reducing manual effort.
8. **Legal and Compliance Considerations**:
   * Ensure that event-based retention policies align with legal and compliance requirements, especially for legal holds.
9. **Monitoring and Reporting**:
   * Regularly review compliance reports to verify that event-based retention is working as intended.
10. **User Training**:
    * Educate users and content owners about event-based retention policies and the events that trigger them.

### Manage the disposition of content in records management

1. **Disposition Overview**:
   * Disposition refers to the process of reviewing, retaining, and ultimately disposing of records according to legal, regulatory, and organizational requirements.
2. **Retention Policies**:
   * Retention labels and policies are used to define how long records should be retained and what actions to take when the retention period ends.
3. **Review and Approval**:
   * Establish procedures for the periodic review and approval of records scheduled for disposition to ensure compliance.
4. **Disposal Actions**:
   * Actions for disposition can include permanent deletion, archival, or transfer to an archive or records management system.
5. **Legal Holds**:
   * Ensure that records under legal holds are not subject to disposition until legal requirements are met.
6. **Disposition Reporting**:
   * Maintain records of disposition actions taken, including what records were disposed of, when, and why.
7. **Auditing and Compliance**:
   * Regularly audit records disposition processes to ensure compliance with policies and regulations.
8. **User Education**:
   * Train users and records managers on the importance of following disposition policies and procedures.
9. **Disposition Automation**:
   * Leverage automation tools to streamline the disposition process, reducing manual effort and errors.
10. **Continuous Improvement**:
    * Continuously assess and refine disposition processes to align with changing legal requirements and business needs.

### Configure records management settings, including retention label settings and disposition settings

1. **Retention Label Settings**:
   * Use the Microsoft 365 Compliance Center to configure retention label settings.
   * Specify label names, descriptions, retention durations, and actions (e.g., delete, retain).
2. **Default Retention Labels**:
   * Microsoft 365 may provide default retention labels, which can be customized or used as-is.
3. **Retention Label Policies**:
   * Define policies that specify where and how retention labels should be applied to content, such as SharePoint sites, OneDrive accounts, or email.
4. **Disposition Settings**:
   * Configure disposition settings to define the actions to be taken when content reaches the end of its retention period.
5. **Disposition Review**:
   * Establish processes for the periodic review and approval of content scheduled for disposition to ensure compliance.
6. **Disposal Actions**:
   * Specify actions for disposition, such as permanent deletion, archival, or transfer to an archive or records management system.
7. **Legal Holds**:
   * Ensure that content under legal holds is exempt from disposition until legal requirements are satisfied.
8. **Automation and Triggers**:
   * Use automation tools to trigger and execute disposition actions automatically, reducing manual effort and human error.
9. **Auditing and Compliance**:
   * Regularly audit and monitor records management settings and processes to ensure compliance with policies and regulations.
10. **User Education**:
    * Educate users, content owners, and administrators about the importance of adhering to records management settings and processes.
11. **Continuous Improvement**:
    * Continuously assess and refine records management settings and processes to align with evolving business requirements and legal standards.

# Monitor and investigate data and activities by using Microsoft Purview (15–20%)

## Plan and manage regulatory requirements by using Microsoft Purview Compliance Manager

### Plan for regulatory compliance in Microsoft 365

**1. Identify Compliance Requirements:**

* Determine the specific regulatory requirements applicable to your organization.
* Understand data protection laws, industry standards, and internal policies.

**2. Data Classification:**

* Categorize data based on sensitivity and regulatory impact.
* Use Microsoft Information Protection to label and protect data accordingly.

**3. Compliance Center:**

* Utilize Microsoft 365 Compliance Center for compliance management.
* Access Compliance Manager to assess compliance posture.

**4. Retention Policies:**

* Define retention policies to retain and dispose of data as per regulatory mandates.
* Implement legal holds when required.

**5. eDiscovery:**

* Use Microsoft 365 eDiscovery to search and identify relevant data for legal purposes.
* Preserve and export data for litigation readiness.

**6. Audit and Monitoring:**

* Enable auditing in Microsoft 365 to track user and admin activities.
* Review audit logs for compliance violations.

**7. Compliance Reports:**

* Generate compliance reports to monitor and demonstrate adherence to regulations.
* Share reports with auditors and stakeholders.

**8. Insider Risk Management:**

* Set up policies to detect and mitigate insider threats.
* Monitor user activities for suspicious behavior.

**9. Compliance Assessments:**

* Conduct compliance assessments to evaluate the effectiveness of controls.
* Address gaps and continuously improve compliance posture.

**10. Data Loss Prevention (DLP):** - Implement DLP policies to prevent unauthorized data sharing. - Customize policies to align with regulatory requirements.

**11. Encryption and Rights Management:** - Use Azure Information Protection to encrypt and protect sensitive data. - Apply rights management to control access and usage.

**12. Third-Party Solutions:** - Integrate third-party compliance solutions if necessary. - Ensure they align with Microsoft 365 compliance capabilities.

**13. Compliance Training:** - Educate employees about compliance policies and practices. - Foster a culture of compliance within the organization.

**14. Regular Updates:** - Stay informed about regulatory changes and updates. - Adjust compliance measures accordingly.

**15. Incident Response:** - Develop an incident response plan for data breaches or non-compliance incidents. - Test and refine the plan regularly.

**16. Documentation and Records:** - Maintain records of compliance efforts and actions taken. - Store documentation securely for auditing purposes.

**17. Compliance Communication:** - Communicate compliance policies and progress to stakeholders. - Ensure transparency and accountability.

**18. Compliance Review Board:** - Establish a compliance review board to oversee and guide compliance efforts. - Include key stakeholders for decision-making.

**19. Continuous Improvement:** - Regularly assess and enhance the compliance program. - Adapt to evolving regulatory landscapes and organizational needs.

**20. Compliance Testing:** - Conduct periodic compliance testing and assessments. - Verify that controls and policies are effective.

### Create and manage assessments

**Overview:**

* Assessments in Microsoft 365 Compliance are used to evaluate and measure compliance with various regulations, standards, and policies.

**Key Concepts:**

1. **Assessment Types:**
   * Microsoft 365 Compliance provides pre-defined assessment templates for common regulations like GDPR, HIPAA, etc.
   * Custom assessments can also be created to address specific organizational requirements.
2. **Creating Assessments:**
   * Navigate to the Security & Compliance Center.
   * Under "Assessment," select "Assessments."
   * Click on "New assessment" to start creating an assessment.
3. **Assessment Settings:**
   * Specify the assessment's name, description, and scope (e.g., locations, users, or devices).
   * Choose the assessment type (standard or custom).
4. **Questions and Controls:**
   * Add questions or controls to the assessment.
   * Customize questions for custom assessments.
   * Associate controls with regulatory requirements.
5. **Scoring and Weighting:**
   * Assign scores or weights to questions/controls based on their importance.
   * Define the pass/fail criteria for assessments.
6. **Assigning Assessments:**
   * Assign assessments to users or groups.
   * Set due dates and reminders.
7. **Assessment Reporting:**
   * Monitor assessment progress and results.
   * Generate reports to view compliance status.
8. **Review and Remediation:**
   * Review assessment results and identify non-compliance areas.
   * Take corrective actions to address compliance gaps.

**Best Practices:**

* Keep assessment questions clear and relevant to the compliance requirements.
* Regularly update and review assessments to adapt to changing compliance needs.
* Communicate assessment objectives and expectations clearly to participants.
* Document assessment results and remediation actions.

**Exam Tips:**

* Understand the purpose and types of assessments.
* Know how to create, configure, and assign assessments.
* Be familiar with scoring, reporting, and remediation processes.
* Practice using the Microsoft 365 Compliance Center for assessment management.

### Create and modify custom templates

**Overview:**

* Custom templates in Microsoft 365 Security are used to define and customize the look and feel of reports and notifications generated by various security services.

**Key Concepts:**

1. **Template Types:**
   * There are two main types of templates: Email Templates and Alert Logic Templates.
2. **Creating Custom Templates:**
   * Navigate to the Security & Compliance Center.
   * Under "Threat management," select "Policy templates."
   * Click on "New custom template" to start creating a template.
3. **Template Settings:**
   * Define template details such as name, description, and severity.
   * Choose which services and scenarios the template applies to.
4. **Template Content:**
   * Customize the email subject, body, and notification content.
   * Use placeholders for dynamic information.
5. **Conditions and Filters:**
   * Set conditions and filters to determine when the template should be triggered.
   * Specify the scope, including locations, users, or devices.
6. **Testing Templates:**
   * Utilize the "Test" feature to preview how the template will appear in notifications.
7. **Modifying Templates:**
   * Edit existing templates by selecting "Edit" from the template list.
   * Modify settings, content, or conditions as needed.
8. **Deleting Templates:**
   * Remove custom templates that are no longer required.
   * Select "Delete" from the template list.

**Best Practices:**

* Use descriptive names and detailed descriptions for templates.
* Regularly review and update templates to reflect changing security needs.
* Test templates thoroughly to ensure they work as intended.
* Document template configurations for reference.

**Exam Tips:**

* Understand the differences between Email Templates and Alert Logic Templates.
* Be familiar with the steps to create, modify, and delete custom templates.
* Know how to customize template content and conditions.
* Practice testing templates to verify their functionality.

### Interpret and manage improvement actions

**Overview:**

* Improvement actions in Microsoft 365 Compliance involve assessing and addressing compliance-related issues and vulnerabilities.

**Key Concepts:**

1. **Assessment Results:**
   * Improvement actions stem from the analysis of assessment results, which identify compliance gaps and issues.
2. **Interpreting Results:**
   * Review assessment findings to understand the nature and severity of compliance deficiencies.
   * Determine the impact on regulatory compliance.
3. **Types of Improvement Actions:**
   * Corrective Actions: Address specific compliance issues identified in assessments.
   * Preventive Actions: Proactively mitigate potential compliance risks.
4. **Managing Improvement Actions:**
   * Create action plans to document the steps required for remediation.
   * Assign responsible individuals or teams to carry out the actions.
5. **Tracking Progress:**
   * Monitor the progress of improvement actions.
   * Use compliance tools and reports to track resolution.
6. **Documentation:**
   * Maintain detailed records of all improvement actions, including their status, completion dates, and any relevant documentation.
7. **Communication:**
   * Keep stakeholders informed about the status of improvement actions and compliance efforts.
8. **Continuous Improvement:**
   * Regularly review and update improvement actions to adapt to changing compliance needs and evolving threats.

**Best Practices:**

* Prioritize improvement actions based on their impact on compliance and risk.
* Clearly define action plans with specific tasks, deadlines, and responsibilities.
* Foster collaboration among teams involved in remediation efforts.
* Document lessons learned and share them to enhance compliance practices.

**Exam Tips:**

* Understand how to interpret assessment results and identify compliance deficiencies.
* Know the difference between corrective and preventive improvement actions.
* Be familiar with the process of creating, assigning, and tracking improvement actions.
* Practice using compliance tools for managing improvement actions.

### Create and manage alert policies for assessments

1. **Alert Policies for Assessments:**
   * Alert policies can be configured specifically for assessment-related events and compliance issues.
2. **Creating Alert Policies:**
   * Navigate to the Security & Compliance Center.
   * Under "Alerts," select "Alert policies."
   * Click on "New alert policy" to create a new policy.
3. **Alert Policy Settings:**
   * Specify the policy name, description, and severity level.
   * Define the assessment events and triggers that will activate the policy.
4. **Conditions and Filters:**
   * Set conditions and filters to narrow down the scope of the alert policy.
   * Configure triggers based on specific assessment criteria or compliance deviations.
5. **Alert Actions:**
   * Determine the actions to be taken when the alert policy is triggered.
   * Actions can include sending notifications, generating reports, or taking automated remediation actions.
6. **Assigning Alert Policies:**
   * Assign alert policies to users, groups, or specific locations within your organization.
   * Ensure relevant personnel receive alerts and notifications.
7. **Monitoring and Responding:**
   * Regularly review alert notifications and assess the impact on compliance.
   * Take appropriate actions to investigate and address alerts promptly.
8. **Alert History and Reporting:**
   * Keep a record of alert history and actions taken.
   * Generate reports to track alert policy effectiveness.

**Best Practices:**

* Tailor alert policies to specific assessment criteria and compliance requirements.
* Regularly review and update alert policies to align with changing compliance needs.
* Establish response workflows to address alerts efficiently.
* Ensure alert policies are well-documented for reference.

**Exam Tips:**

* Understand the purpose and use of alert policies for assessments.
* Know how to create, configure, and assign alert policies.
* Be familiar with conditions, triggers, and alert actions.
* Practice monitoring and responding to alerts within the Microsoft 365 Compliance Center.

## Plan and manage eDiscovery and Content search

### Choose between eDiscovery (Standard) and eDiscovery (Premium) based on an organization’s requirements

**Overview:**

* Microsoft 365 offers both eDiscovery (Standard) and eDiscovery (Premium) solutions for organizations to manage and search for electronic content, particularly for legal and compliance purposes.

**Key Considerations:**

1. **eDiscovery (Standard):**
   * Basic eDiscovery capabilities included in most Microsoft 365 plans.
   * Suitable for organizations with relatively straightforward compliance and legal requirements.
   * Provides core eDiscovery features such as content search, legal holds, and exporting data.
   * Limited to searching content in Exchange Online, SharePoint Online, and OneDrive for Business.
2. **eDiscovery (Premium):**
   * Part of Microsoft 365 Compliance Center and available as a separate subscription.
   * Ideal for organizations with complex compliance needs, large datasets, or international legal requirements.
   * Offers advanced features like:
     + Advanced eDiscovery: Allows for more complex searches, machine learning, and analytics.
     + Case Management: Organizes eDiscovery cases, workflows, and collaboration.
     + Content Search across more services: Expands search capabilities to Teams, Yammer, and more.
     + Export with more options: Supports exporting data in various formats and provides better control.
     + Custodian Management: More granular control over data sources and preservation.

**Choosing Between Them:**

* **Select eDiscovery (Standard) If:**
  + Your organization has basic eDiscovery needs.
  + You primarily use Exchange Online, SharePoint Online, and OneDrive for Business.
  + Budget constraints are a concern.
* **Choose eDiscovery (Premium) If:**
  + Your organization has complex or international compliance requirements.
  + You work with large datasets that require advanced search and analytics.
  + You need case management features for organizing and tracking legal matters.
  + You use additional services beyond the core Microsoft 365 applications.

**Best Practices:**

* Evaluate your organization's specific eDiscovery needs and regulatory obligations.
* Consider data volume, search complexity, and the need for advanced analytics.
* Budget constraints may influence your decision, but prioritize compliance requirements.

**Exam Tips:**

* Understand the differences between eDiscovery (Standard) and eDiscovery (Premium).
* Be able to identify scenarios where one solution is more suitable than the other.
* Consider cost implications and compliance requirements when choosing between the two options.

### Plan and implement eDiscovery

* eDiscovery in Microsoft 365 is the process of identifying, preserving, and collecting electronic information for legal and compliance purposes.

**Key Steps:**

1. **Assessment:**
   * Identify the specific legal and compliance requirements of your organization.
   * Understand the scope and nature of eDiscovery needs.
2. **Plan eDiscovery:**
   * Determine which eDiscovery solution to use (eDiscovery Standard or Premium).
   * Define roles and responsibilities for eDiscovery team members.
   * Create a strategy for data preservation, collection, and analysis.
3. **Data Sources:**
   * Identify relevant data sources such as Exchange Online, SharePoint, OneDrive, Teams, and more.
   * Consider external data sources, if applicable.
4. **Legal Holds:**
   * Implement legal holds to ensure that data subject to litigation or investigations is preserved and not deleted.
   * Use eDiscovery tools to place holds on specific data.
5. **Search and Collection:**
   * Create search queries to identify and collect relevant data.
   * Use eDiscovery tools to perform content searches and export data for analysis.
6. **Analysis and Review:**
   * Review collected data for relevance and legal privilege.
   * Collaborate with legal teams and use advanced eDiscovery tools for analysis.
7. **Export and Production:**
   * Export relevant data in the required format.
   * Ensure proper chain of custody and documentation for produced data.
8. **Reporting and Documentation:**
   * Maintain detailed records of the eDiscovery process, including actions taken and decisions made.
   * Generate reports for legal and compliance purposes.
9. **Data Privacy and Security:**
   * Ensure compliance with data protection regulations during eDiscovery.
   * Safeguard sensitive information throughout the process.
10. **Testing and Validation:**
    * Test eDiscovery processes and procedures to ensure they work effectively.
    * Validate that legal holds, searches, and exports meet compliance requirements.

**Best Practices:**

* Collaborate closely with legal teams to align eDiscovery processes with legal requirements.
* Regularly update and test eDiscovery procedures to adapt to changing regulations.
* Maintain a clear and organized record of all eDiscovery activities.

**Exam Tips:**

* Understand the eDiscovery process from assessment to reporting.
* Differentiate between eDiscovery Standard and Premium features.
* Be aware of data sources, legal holds, search queries, and export procedures.
* Practice using Microsoft 365 eDiscovery tools within the Compliance Center.

### Delegate permissions to use eDiscovery and Content search

**Overview:**

* Delegating permissions for eDiscovery and Content Search in Microsoft 365 allows specific users or roles to perform these tasks without granting excessive access.

**Key Concepts:**

1. **Role-Based Access Control (RBAC):**
   * RBAC is used to assign permissions in Microsoft 365.
   * It provides fine-grained control over who can perform eDiscovery and Content Search tasks.
2. **Built-in Roles:**
   * Microsoft 365 includes several built-in roles for eDiscovery and Content Search, such as "eDiscovery Manager" and "eDiscovery Administrator."
3. **Custom Roles:**
   * Organizations can create custom roles with specific permissions tailored to their needs.
   * Custom roles can be more granular than built-in roles.
4. **Assigning Permissions:**
   * Permissions can be assigned at various levels, including organization-wide or specific to a scope, such as a mailbox or site collection.
5. **eDiscovery Permissions:**
   * Users with eDiscovery permissions can create, modify, and delete eDiscovery cases, legal holds, and content searches.
6. **Content Search Permissions:**
   * Users with Content Search permissions can create and manage content search queries and export search results.

**Steps to Delegate Permissions:**

1. **Access Permissions:**
   * Navigate to the Microsoft 365 admin center or Security & Compliance Center.
2. **Role Assignment:**
   * Assign roles to users or groups by selecting the role and specifying the scope (e.g., users, locations, or groups).
3. **Custom Roles (Optional):**
   * If using custom roles, create the role with specific permissions, and then assign it to users or groups.
4. **Review and Test:**
   * Carefully review permissions to ensure they align with organizational needs.
   * Test delegated users' access to verify that permissions work as intended.

**Best Practices:**

* Follow the principle of least privilege when delegating permissions.
* Regularly review and update delegated permissions based on personnel changes and evolving requirements.
* Document and communicate delegated access to ensure clarity and compliance.

**Exam Tips:**

* Understand the role of RBAC in delegating permissions for eDiscovery and Content Search.
* Be aware of built-in and custom roles available for these tasks.
* Know the steps to assign and test delegated permissions.

### Perform searches and respond to results from eDiscovery

**Overview:**

* In Microsoft 365 Compliance, performing searches and responding to results from eDiscovery involves searching for electronic content, analyzing findings, and taking appropriate actions to comply with legal and regulatory requirements.

**Key Concepts:**

1. **Content Searches:**
   * Content searches involve querying data repositories for specific content relevant to legal or compliance matters.
   * Searches can target emails, documents, chats, and other forms of electronic information.
2. **eDiscovery Cases:**
   * eDiscovery cases are containers used to organize and manage the eDiscovery process.
   * Cases help track searches, holds, and exports related to a specific legal or compliance matter.
3. **Search Queries:**
   * Search queries are defined criteria that determine what content is sought in an eDiscovery search.
   * Queries can be simple keyword searches or complex, using operators and conditions.
4. **Exporting Data:**
   * Exporting data is the process of extracting and preserving search results for legal or compliance purposes.
   * Exported data may be needed for review, analysis, or sharing with legal teams.
5. **Legal Holds:**
   * Legal holds are used to preserve data relevant to a legal or regulatory matter.
   * Data under legal hold cannot be deleted until the hold is released.

**Steps to Perform Searches and Respond to Results:**

1. **Create an eDiscovery Case:**
   * Start by creating an eDiscovery case for the specific legal or compliance matter.
2. **Define Search Criteria:**
   * Create search queries that specify what content to search for within the case.
3. **Initiate the Search:**
   * Run the search using the defined criteria.
   * Monitor the progress of the search.
4. **Review Search Results:**
   * Analyze the search results to determine relevance and legal privilege.
   * Mark items for further action, such as export or placing on legal hold.
5. **Export Data:**
   * Export the search results in the required format.
   * Ensure proper documentation and chain of custody for the exported data.
6. **Manage Legal Holds:**
   * Place data relevant to the case on legal hold.
   * Regularly review and release holds when they are no longer necessary.
7. **Report and Documentation:**
   * Maintain detailed records of the eDiscovery process, including search criteria, results, and actions taken.
   * Generate reports for legal and compliance purposes.

**Best Practices:**

* Collaborate closely with legal teams to ensure searches and responses meet legal requirements.
* Document and communicate eDiscovery processes and findings clearly.
* Keep records organized and up-to-date to facilitate audits and legal reviews.

**Exam Tips:**

* Understand the steps involved in performing eDiscovery searches and responding to results.
* Familiarize yourself with the concept of eDiscovery cases, search queries, legal holds, and data export.
* Be prepared to demonstrate the ability to manage eDiscovery processes using Microsoft 365 Compliance Center.

### Manage eDiscovery cases

* Managing eDiscovery cases in Microsoft 365 involves creating, organizing, and overseeing the process of collecting and preserving electronic information for legal and compliance purposes.

**Key Concepts:**

1. **eDiscovery Cases:**
   * eDiscovery cases are containers that organize and manage the eDiscovery process for specific legal or compliance matters.
   * Each case represents a distinct investigation or litigation scenario.
2. **Case Settings:**
   * When creating an eDiscovery case, configure settings such as the case name, description, and scope.
   * Scope defines the data sources and locations where eDiscovery actions will apply.
3. **Assign Permissions:**
   * Specify who can access and manage the eDiscovery case by assigning roles and permissions.
   * Roles like "eDiscovery Manager" and "eDiscovery Administrator" control access.
4. **Content Searches:**
   * Create content search queries within the eDiscovery case to identify relevant electronic content.
   * Content searches are used to collect data for further analysis.
5. **Legal Holds:**
   * Legal holds are used to preserve data relevant to the eDiscovery case.
   * Data under hold cannot be deleted until the hold is released.
6. **Export and Review:**
   * Export data from the case for legal review and analysis.
   * Review search results and take appropriate actions based on findings.

**Steps to Manage eDiscovery Cases:**

1. **Create a New eDiscovery Case:**
   * Start by creating a new eDiscovery case and configure its settings.
2. **Assign Permissions:**
   * Specify who can access and manage the case by assigning appropriate roles and permissions.
3. **Define the Case Scope:**
   * Define the scope of the case, specifying data sources, locations, and users involved.
4. **Create Content Search Queries:**
   * Develop content search queries within the case to identify relevant content.
5. **Initiate Searches:**
   * Run the content searches to collect data based on the defined criteria.
6. **Manage Legal Holds:**
   * Place data relevant to the case under legal hold to prevent deletion.
7. **Export Data:**
   * Export the collected data for further legal review or analysis.
8. **Monitor and Review:**
   * Regularly monitor the case, review search results, and take actions as needed.
9. **Release Legal Holds:**
   * Once the case is concluded, release legal holds to allow data deletion as necessary.

**Best Practices:**

* Collaborate closely with legal teams to ensure eDiscovery cases align with legal requirements.
* Document case details, actions taken, and findings for compliance and auditing purposes.
* Keep eDiscovery cases organized and clearly labeled for easy reference.

**Exam Tips:**

* Understand the purpose and components of eDiscovery cases.
* Be familiar with case settings, permissions, content searches, legal holds, and data export within eDiscovery cases.
* Practice managing eDiscovery cases using the Microsoft 365 Compliance Center.

### Perform searches by using Content search

**Overview:**

* Content search in Microsoft 365 allows you to search for specific content within your organization's data repositories for various purposes, including compliance, investigations, and legal requirements.

**Key Concepts:**

1. **Content Search Purpose:**
   * Content search is used to locate and retrieve electronic information, such as emails, documents, and chats, that match specific criteria.
2. **Search Queries:**
   * Search queries define the criteria for the content search, specifying keywords, sender/recipients, date ranges, and more.
   * Queries can be simple or complex, using logical operators and conditions.
3. **Search Scopes:**
   * Content searches can be scoped to specific data sources, such as Exchange Online, SharePoint, OneDrive, Teams, and more.
   * Scoping helps narrow down the search to relevant data.
4. **Search Preview:**
   * Before executing a content search, you can preview the search results to ensure they align with your expectations.
5. **Search Filters:**
   * Filters allow you to further refine search results based on criteria like file types, sender domains, or message classes.

**Steps to Perform Content Search:**

1. **Access the Content Search Tool:**
   * Navigate to the Microsoft 365 Compliance Center or use PowerShell cmdlets for advanced searches.
2. **Create a New Content Search:**
   * Start by creating a new content search query.
3. **Define Search Criteria:**
   * Specify search criteria, such as keywords, date ranges, and data sources.
   * Use logical operators like AND, OR, NOT for complex queries.
4. **Scope the Search:**
   * Choose the data sources and locations where the search should be performed.
   * Define the scope to target specific data repositories.
5. **Preview the Search:**
   * Before running the search, preview the results to ensure they match your intended criteria.
6. **Execute the Search:**
   * Run the content search query to collect relevant data.
7. **Review and Export Results:**
   * Review the search results and take actions, such as exporting data for further analysis or compliance purposes.

**Best Practices:**

* Plan content searches carefully, focusing on specific criteria to avoid excessive data retrieval.
* Test search queries in a controlled environment to avoid unintended consequences.
* Document search criteria, results, and actions taken for compliance and legal purposes.

**Exam Tips:**

* Understand the purpose and process of content search in Microsoft 365.
* Be familiar with search query creation, scoping, and previewing.
* Practice performing content searches using the Microsoft 365 Compliance Center.

## Manage and analyze audit logs and reports in Microsoft Purview

### Choose between Audit (Standard) and Audit (Premium) based on an organization’s requirements

**Audit (Standard):**

* Basic auditing capabilities.
* Suitable for smaller organizations with simpler compliance needs.
* Provides essential audit trail for data activities.
* Limited customization and retention options.
* Cost-effective option for basic auditing requirements.

**Audit (Premium):**

* Advanced auditing features.
* Ideal for large organizations with complex compliance needs.
* Offers extensive customization and retention settings.
* Enhanced monitoring and alerting capabilities.
* Higher cost but comprehensive compliance coverage.

In summary, select Audit (Standard) for basic needs and cost-effectiveness, while Audit (Premium) is best for advanced compliance demands and robust customization. Tailor your choice to your organization's specific requirements.

### Plan for and configure auditing

* **Auditing Purpose**: Auditing helps track and analyze activities within Purview for security and compliance.
* **Audit Logs**: Purview generates audit logs for various actions, including data access, administrative changes, and more.
* **Auditing Levels**:
  + **Azure Monitor Logs**: Basic level auditing for essential activities.
  + **Audit (Standard)**: Enhanced auditing for detailed data access tracking.
  + **Audit (Premium)**: Advanced auditing with extended retention and customization.
* **Configuration Steps**:
  + **Access Control (IAM)**: Assign proper roles for users to access auditing settings.
  + **Purview Studio**: Configure audit settings through the Purview Studio.
  + **Audit Categories**: Define which categories of activities to audit (e.g., data access, administrative actions).
  + **Retention Period**: Specify how long to retain audit logs.
  + **Export Logs**: Choose destinations (e.g., Azure Storage, Event Hubs) to export audit logs for analysis.
* **Compliance Requirements**: Align auditing configurations with organizational compliance needs and industry standards.
* **Monitoring and Alerts**: Implement real-time monitoring and alerts for critical audit events to proactively address issues.
* **Testing**: Regularly test audit configurations to ensure they function as expected and meet compliance requirements.

### Investigate activities by using the unified audit log

* **Unified Audit Log**: A centralized repository of audit events from various Microsoft services, including Purview.
* **Purpose**: Used to investigate and analyze user and admin activities for security, compliance, and troubleshooting.
* **Accessing Unified Audit Log**:
  1. **Microsoft 365 Compliance Center**: Primary interface for accessing and searching the unified audit log.
  2. **PowerShell**: Use PowerShell cmdlets to query and export audit data programmatically.
* **Audit Data Details**:
  1. Includes information on who, what, when, and where (IP addresses).
  2. Tracks actions like file access, logins, sharing, and administrative changes.
* **Search and Filter**:
  1. Utilize search criteria (e.g., date, user, activity) to narrow down results.
  2. Apply filters to focus on specific audit events of interest.
* **Export and Analysis**:
  1. Export audit data for further analysis, compliance reporting, or legal requirements.
  2. Analyze patterns and anomalies to identify potential security issues.
* **Alerting**:
  1. Set up alerts based on specific audit events to receive notifications for critical activities.
* **Retention Policies**:
  1. Configure retention policies to control how long audit logs are stored to meet compliance requirements.
* **Use Cases**:
  1. Investigate data breaches or unauthorized access.
  2. Monitor compliance with organizational policies.
  3. Troubleshoot technical issues and errors.

In summary, the unified audit log in Microsoft Purview provides a comprehensive view of activities, enabling organizations to investigate and respond to security incidents, ensure compliance, and troubleshoot operational issues effectively.

### Review and interpret compliance reports and dashboards

* **Compliance Reports and Dashboards**: Tools for assessing and managing data compliance within Microsoft Purview.
* **Purpose**: Monitor adherence to regulatory standards, internal policies, and data protection requirements.
* **Key Components**:
  1. **Compliance Center**: Central hub for accessing compliance reports and dashboards.
  2. **Reports**: Pre-defined and customizable reports that provide insights into data compliance.
  3. **Dashboards**: Visual representations of compliance data, often with drill-down capabilities.
* **Common Compliance Standards**:
  1. GDPR, HIPAA, CCPA, etc., depending on regional and industry-specific requirements.
* **Data Classification**:
  1. Classify data based on sensitivity levels to track compliance more effectively.
* **Data Loss Prevention (DLP)**:
  1. Monitor and prevent unauthorized data sharing or leakage through DLP policies.
* **Audit Logs**:
  1. Review audit logs to ensure compliance with data access and usage policies.
* **Alerts and Notifications**:
  1. Configure alerts to be notified of compliance violations in real-time.
* **Customization**:
  1. Tailor reports and dashboards to align with specific compliance needs and organizational goals.
* **Compliance Score**:
  1. Measure and improve compliance posture with Compliance Score metrics and recommendations.
* **Use Cases**:
  1. Assess compliance with data protection regulations.
  2. Identify and mitigate compliance risks.
  3. Demonstrate compliance to auditors and stakeholders.
  4. Continuously monitor and improve compliance posture.

### Configure alert policies

* **Alert Policies**: Settings that trigger notifications or automated actions in response to specific events or conditions in Microsoft Purview.
* **Purpose**: Enhance security, compliance, and monitoring by proactively addressing potential issues.
* **Configuration Steps**:
  1. **Access Policies**: Determine who can create and manage alert policies.
  2. **Alert Conditions**: Define criteria or triggers for alerts (e.g., failed logins, data breaches).
  3. **Actions**: Specify actions to take when an alert is triggered (e.g., email notification, run a script).
  4. **Alert Severity**: Assign severity levels to prioritize responses.
  5. **Notifications**: Set up notification channels for alert delivery (e.g., email, SMS).
  6. **Retention**: Define how long alert data should be retained for analysis and reporting.
* **Use Cases**:
  1. **Security**: Detect and respond to suspicious activities or security breaches.
  2. **Compliance**: Ensure adherence to data protection and regulatory requirements.
  3. **Operational**: Monitor system health, performance, and resource utilization.
* **Alert Sources**:
  1. **Logs and Audit Data**: Utilize audit logs and event data as sources for alert policies.
  2. **Azure Monitor**: Integrate with Azure Monitor for advanced alerting capabilities.
* **Alert Automation**:
  1. Automate responses with remediation scripts or runbooks to address issues swiftly.
* **Testing and Validation**:
  1. Regularly test alert policies to ensure they function as intended.
* **Alert Lifecycle**:
  1. Alert creation, detection, notification, investigation, resolution, and closure.
* **Continuous Improvement**:
  1. Review and adjust alert policies based on evolving threats and organizational needs.

### Configure audit retention policies

* **Audit Retention Policies**: Settings that determine how long audit logs and data are retained in Microsoft Purview.
* **Purpose**: To meet compliance, legal, and security requirements by preserving audit data for a specified duration.
* **Configuration Steps**:
  1. **Access Audit Settings**: Access Purview Studio or Azure portal to configure audit retention.
  2. **Select Scope**: Define the scope of audit retention (e.g., organization-wide or specific resources).
  3. **Retention Period**: Specify the duration for which audit data should be retained.
  4. **Archive or Delete**: Decide whether to archive or permanently delete data after retention.
* **Considerations**:
  1. Align retention policies with legal and compliance requirements (e.g., GDPR, HIPAA).
  2. Different types of data may have varying retention needs.
* **Impact on Storage**:
  1. Longer retention periods can increase storage costs.
  2. Consider cost implications when defining retention policies.
* **Compliance Audits**:
  1. Regularly review and update audit retention policies to ensure compliance.
* **Use Cases**:
  1. **Compliance**: Maintain audit data for regulatory compliance and audit trails.
  2. **Security**: Preserve data for investigating security incidents and unauthorized access.
  3. **Analysis**: Retain data for historical analysis and trend identification.
* **Data Privacy**: Ensure that retained data complies with data privacy regulations regarding data subject rights and deletion.
* **Testing**: Periodically test the retrieval and access to retained audit data to verify policy effectiveness.

# Manage insider and privacy risk in Microsoft 365 (15–20%)

## Implement and manage Microsoft Purview Communication Compliance

### Plan for communication compliance

* **Communication Compliance**: A feature in Microsoft Purview for monitoring and ensuring compliance in electronic communications.
* **Purpose**: To proactively identify and address policy violations, sensitive data leaks, and inappropriate content.
* **Key Components**:
  1. **Policy Configuration**: Define communication compliance policies based on organizational requirements.
  2. **Content Analysis**: Monitor communication content for policy violations and sensitive information.
  3. **Alerts and Notifications**: Receive real-time alerts for policy breaches.
  4. **Review and Investigation**: Review flagged content and take necessary actions.
  5. **Archiving and Retention**: Ensure proper retention and retrieval of communication data.
* **Policy Creation**:
  1. Specify which communications channels and users to monitor.
  2. Define policy rules for content, keywords, and violations.
  3. Set actions for detected violations (e.g., notify, block, quarantine).
* **Use Cases**:
  1. **Data Leakage Prevention**: Prevent the unauthorized sharing of sensitive data.
  2. **Compliance Monitoring**: Ensure communications adhere to regulatory standards.
  3. **Ethical Conduct**: Monitor for harassment, bullying, or inappropriate content.
  4. **Security Threats**: Detect and respond to security threats in communications.
* **Data Sources**:
  1. Communication compliance can analyze data from various sources, including email, chat, and social media.
* **Retention and Legal Requirements**:
  1. Ensure compliance with retention and legal requirements for monitored communications.
* **Integration with Other Tools**:
  1. Integrate communication compliance with other security and compliance tools for a holistic approach.
* **Continuous Monitoring**:
  1. Regularly review policies and adjust them to evolving compliance needs.

### Create and manage communication compliance policies

* **Communication Compliance Policies**: Rules and configurations in Microsoft Purview to monitor and enforce communication standards.
* **Purpose**: To ensure adherence to organizational policies, regulatory requirements, and ethical standards in electronic communications.
* **Configuration Steps**:

1. **Access Compliance Center**: Sign in to Microsoft 365 Compliance Center to create and manage policies.
2. **Create a Policy**:
   * Choose policy type (e.g., Anti-harassment, Data Loss Prevention).
   * Define scope (users, groups, communication channels).
   * Specify policy rules, conditions, and actions for violations.
3. **Content Analysis**:
   * Use predefined templates or customize rules to scan communication content.
   * Define keywords, phrases, or patterns to identify policy violations.
4. **Actions for Violations**:
   * Determine what actions to take when policy violations are detected (e.g., notify, block, quarantine).
5. **Review and Alerts**:
   * Configure alerts to be notified of policy breaches in real-time.
   * Designate reviewers to assess flagged content.
6. **Review and Investigation**:
   * Review and investigate flagged communication for policy violations.
   * Take necessary actions, such as warning users or escalating issues.
7. **Policy Testing**:
   * Conduct testing to ensure policies are effective and not overly restrictive.

* **Use Cases**:
  + **Data Protection**: Prevent unauthorized data sharing and protect sensitive information.
  + **Compliance**: Ensure electronic communications comply with industry regulations (e.g., GDPR, HIPAA).
  + **Ethical Conduct**: Monitor for inappropriate content, harassment, or cyberbullying.
* **Policy Scope**:
  + Policies can apply to various communication channels, including email, chat, and social media.
* **Continuous Management**:
  + Regularly review and update policies to align with changing compliance needs and emerging threats.

### Investigate and remediate communication compliance alerts and reports

1. **Communication Compliance in Purview:**
   * Purview includes a Communication Compliance feature for monitoring and managing communication within an organization.
2. **Alerts and Reports:**
   * Communication Compliance provides alerts and reports to help organizations maintain compliance with communication policies.
3. **Alerts Overview:**
   * Alerts are notifications generated when potential policy violations are detected.
   * Alerts can be related to emails, chats, or other communication platforms.
   * They are based on predefined or custom policies.
4. **Investigating Alerts:**
   * Access the Purview portal and navigate to the Communication Compliance dashboard.
   * Review the list of alerts to prioritize investigations.
   * Click on an alert to view details, including the violating content and affected users.
5. **Remediation Actions:**
   * Take appropriate remediation actions based on the severity of the alert.
   * Actions may include warning the user, disabling a feature, or escalating to a higher authority.
6. **Alerts Workflow:**
   * Follow the established workflow for handling alerts, which may involve collaboration with HR, legal, or IT teams.
7. **Reports Overview:**
   * Communication Compliance provides detailed reports on compliance activities.
   * Reports can be customized and scheduled for regular review.
8. **Customizing Reports:**
   * Customize reports to focus on specific compliance metrics or time frames.
   * Export reports for further analysis or sharing with stakeholders.
9. **Policy Fine-Tuning:**
   * Regularly review and fine-tune communication compliance policies to adapt to changing organizational needs.
10. **Training and Awareness:**
    * Promote awareness among employees about communication compliance policies and consequences.
11. **Continuous Monitoring:**
    * Establish ongoing monitoring to ensure compliance and address emerging issues promptly.
12. **Documentation:**
    * Maintain records of investigations, actions taken, and compliance reports for auditing purposes.
13. **Integration:**
    * Purview Communication Compliance can be integrated with other Microsoft 365 services for a holistic approach to compliance management.

## Implement and manage Microsoft Purview Insider Risk Management

### Plan for insider risk management

1. **Overview**: Insider risk management focuses on identifying and addressing threats from within an organization, such as data leaks or unauthorized access.
2. **Purview Integration**: Purview integrates with Microsoft 365 Insider Risk Management to centralize data for analysis.
3. **Identifying Risks**: Use Purview to collect data from various sources, like emails and file activity, to identify potential risks.
4. **Configuration**: Configure Purview to analyze data based on custom risk indicators, such as suspicious file access or employee behavior.
5. **Policy Creation**: Develop policies for insider risk detection, defining thresholds and actions for different risk levels.
6. **Alerts and Notifications**: Configure alerts and notifications to inform stakeholders about potential insider risks in real-time.
7. **Incident Management**: Establish procedures for responding to insider risk incidents, including investigation and remediation steps.
8. **User Training**: Provide training to employees on data security and compliance to reduce unintentional insider risks.
9. **Continuous Monitoring**: Use Purview to continuously monitor insider risks and adapt policies as needed.
10. **Compliance**: Ensure that insider risk management aligns with regulatory compliance requirements, like GDPR or HIPAA.
11. **Data Loss Prevention (DLP)**: Integrate Purview with Microsoft DLP to enhance data protection and reduce insider risk.
12. **Reporting and Analytics**: Utilize Purview's reporting and analytics capabilities to track insider risk trends and improvements over time.

### Create and manage insider risk management policies

1. **Policy Creation**: To create policies, go to Microsoft 365 Security Center.
2. **Policy Types**: You can create Activity, Content, or Policy Query-based policies.
3. **Activity Policies**: Monitor user and entity behavior, such as file sharing, printing, or data access.
4. **Content Policies**: Focus on specific data types or sensitive content. Define criteria for detection.
5. **Policy Query-based Policies**: Use custom queries to identify risky activities or content.
6. **Conditions**: Set conditions to trigger policy actions, like when sensitive data is shared externally.
7. **Policy Actions**: Define actions for policy matches, including email notifications, user activity blocking, or custom scripts.
8. **Alerts**: Configure alerts to notify stakeholders when policies are violated.
9. **Incident Management**: Establish processes for handling incidents detected by policies.
10. **Policy Testing**: Test policies before deploying them to ensure they work as intended.
11. **Continuous Monitoring**: Policies should be regularly reviewed and updated to adapt to changing risks.
12. **Policy Enforcement**: Enforce policies to mitigate insider risks effectively.
13. **Compliance Considerations**: Ensure policies align with regulatory compliance requirements.
14. **Integration**: Integrate with other Microsoft 365 services, like DLP, to enhance policy effectiveness.
15. **Documentation**: Maintain documentation for policies and procedures for auditing purposes.

### Investigate and remediate insider risk activities, alerts, and reports

1. **Activity Investigation**: Start investigations in the Microsoft 365 Security Center.
2. **Alerts Review**: Regularly review alerts generated by insider risk policies.
3. **Alert Details**: Examine alert details, including affected users, activity, and severity.
4. **Alert Resolution**: Take appropriate actions based on alerts, like user warnings, suspensions, or terminations.
5. **User Activity Timeline**: Utilize the user activity timeline to understand context and investigate further.
6. **Evidence Collection**: Collect evidence related to the insider risk incident for documentation and analysis.
7. **Data Export**: Export relevant data for further analysis or legal purposes.
8. **Case Management**: Create cases for detailed investigation of insider risk incidents.
9. **Collaboration**: Collaborate with relevant teams, such as legal or HR, during investigations.
10. **Remediation**: Apply remediation measures to mitigate risks, such as revoking access or changing permissions.
11. **Report Generation**: Generate reports summarizing investigation findings and actions taken.
12. **Documentation**: Maintain detailed records of investigations and remediation efforts.
13. **Audit Trails**: Ensure compliance with audit trail requirements during the investigation.
14. **Continuous Monitoring**: Regularly monitor and reassess risks even after remediation.
15. **Training and Awareness**: Consider employee training and awareness programs to prevent future insider risks.

### Manage insider risk cases

1. **Case Creation**: Initiate cases in the Microsoft 365 Security Center for insider risk incidents.
2. **Case Details**: Provide relevant information about the incident, including affected users, severity, and context.
3. **Assigning Ownership**: Assign a case owner responsible for overseeing the investigation and resolution.
4. **Investigation Steps**: Outline investigation steps and strategies to address the insider risk incident.
5. **Collaboration**: Collaborate with relevant teams, such as legal, HR, or IT, to gather information and insights.
6. **Evidence Collection**: Collect and preserve evidence related to the insider risk case for documentation.
7. **Communication**: Maintain clear and timely communication with stakeholders throughout the case.
8. **Remediation Actions**: Implement remediation measures to mitigate risks and prevent future incidents.
9. **Case Updates**: Regularly update the case status, findings, and actions taken.
10. **Closure**: Close the case once the investigation is complete and risks are adequately addressed.
11. **Documentation**: Thoroughly document all aspects of the case, including findings and resolutions.
12. **Reporting**: Generate reports summarizing the case details, actions, and outcomes.
13. **Legal Considerations**: Ensure compliance with legal and regulatory requirements during case management.
14. **Continuous Monitoring**: Continue monitoring for potential insider risks even after case closure.
15. **Lessons Learned**: Conduct post-case reviews to identify lessons and improve future risk management.

### Manage forensic evidence settings

1. **Forensic Evidence**: Refers to digital artifacts collected during investigations.
2. **Evidence Settings**: Configure settings to collect and manage forensic evidence effectively.
3. **Evidence Sources**: Define sources of evidence, such as email, file activity, or user behavior.
4. **Data Retention**: Set retention policies to determine how long evidence is stored.
5. **Evidence Collection**: Automate evidence collection to ensure timely retrieval of relevant data.
6. **Customization**: Tailor evidence settings to specific investigation requirements.
7. **Legal Compliance**: Ensure evidence handling aligns with legal and regulatory standards.
8. **Chain of Custody**: Maintain a clear chain of custody for all collected evidence.
9. **Data Protection**: Implement encryption and access controls to safeguard forensic data.
10. **Evidence Analysis**: Utilize collected evidence for thorough investigation and reporting.
11. **Documentation**: Document evidence collection and handling procedures for audits.
12. **Secure Storage**: Store forensic evidence in secure and tamper-proof environments.
13. **Access Controls**: Restrict access to forensic evidence to authorized personnel.
14. **Audit Trails**: Maintain audit trails to track who accessed and modified evidence.
15. **Data Disposal**: Ensure proper disposal of evidence when retention periods expire.

### Manage notice templates

1. **Notice Templates**: These are predefined messages used to communicate with users during insider risk investigations.
2. **Customization**: Modify notice templates to align with investigation needs and company policies.
3. **Use Cases**: Notice templates are typically used to inform users about potential policy violations or data access alerts.
4. **Content**: Include clear and informative content in templates, specifying the issue and required actions.
5. **Personalization**: Customize templates with user-specific information, such as their name or specific actions needed.
6. **Translation**: Ensure templates are available in multiple languages if your organization operates globally.
7. **Preview**: Review templates before sending to ensure accuracy and clarity.
8. **Testing**: Test templates to confirm they work as intended in the investigation workflow.
9. **Documentation**: Maintain records of template modifications and usage for auditing purposes.
10. **Legal Compliance**: Ensure that notice templates comply with legal and regulatory requirements.
11. **Communication**: Use templates to communicate effectively with users involved in an investigation.
12. **Consistency**: Maintain consistency in the tone and style of notice templates across different cases.

## Implement and manage Microsoft Purview Information Barriers (IBs)

### Plan for IBs

1. **Information Barriers (IBs)**: IBs are policies that restrict communication and data access between specific groups within an organization.
2. **Use Cases**: IBs are used to meet compliance requirements, prevent conflicts of interest, and maintain data segregation.
3. **Policy Definition**: Define IB policies to specify which groups cannot communicate or share data.
4. **Communication Segregation**: Ensure that members of restricted groups cannot send emails or messages to each other.
5. **Data Segregation**: Implement IBs to prevent restricted groups from accessing each other's data.
6. **Policy Enforcement**: Policies should be enforced consistently to maintain compliance and security.
7. **Exceptions**: Define exceptions for specific scenarios where communication or data sharing is necessary.
8. **Testing**: Test IB policies to verify that they work as intended and do not hinder essential communication.
9. **Monitoring**: Continuously monitor and update IB policies to adapt to organizational changes.
10. **Documentation**: Maintain documentation of IB policies and exceptions for auditing purposes.
11. **Compliance**: Ensure IBs align with relevant industry regulations and legal requirements.
12. **User Training**: Provide training to users to make them aware of IB policies and their implications.

### Create and manage IB segments and policies

**IB Segments (Information Barriers):**

* **Definition:** Information Barriers (IB) segments in Microsoft Purview are used to control communication between different groups within an organization to prevent conflicts of interest or compliance violations.
* **Creation:** To create an IB Segment:
  1. Navigate to Purview Admin Portal.
  2. Go to Information Barriers.
  3. Click "Segments" and select "New Segment."
  4. Define the segment's name, description, and members.
  5. Save the segment.
* **Membership:** Segments can include users or groups. Ensure that members are assigned appropriately to enforce communication restrictions.

**IB Policies (Information Barriers):**

* **Definition:** IB Policies in Microsoft Purview are used to specify the rules and actions for controlling communication between different segments.
* **Creation:** To create an IB Policy:
  1. Navigate to Purview Admin Portal.
  2. Go to Information Barriers.
  3. Click "Policies" and select "New Policy."
  4. Define the policy's name, description, and conditions.
  5. Specify the actions to be taken when conditions are met.
  6. Save the policy.
* **Conditions:** Conditions can be based on user attributes, keywords, or specific content.
* **Actions:** Actions can include blocking communication, sending notifications, or logging events.

**Managing IB Segments and Policies:**

* **Editing Segments/Policies:** To modify segments or policies, navigate to the respective section in the Purview Admin Portal, select the item, and click "Edit."
* **Disabling Segments/Policies:** You can temporarily disable segments or policies by selecting the item and choosing "Disable."
* **Monitoring:** Regularly monitor IB segments and policies for compliance and effectiveness.
* **Testing:** Before enforcing IB policies, consider testing them in a controlled environment to ensure they work as intended.

**Best Practices:**

* Clearly define segment membership criteria.
* Keep policies concise and focused on specific compliance or security requirements.
* Regularly review and update segments and policies as organizational needs change.

### Configure Teams, SharePoint, and OneDrive to enforce IBs, including setting barrier modes

**Information Barriers (IB) Enforcement:**

* **Definition:** IB enforcement in Microsoft Purview ensures that communication and data sharing between different segments are compliant with organizational policies.

**Configuring Teams for IBs:**

* **Barrier Modes:** Teams supports two barrier modes for IB enforcement:
  1. **Allow List Mode:** Allows communication only between specified segments.
  2. **Block List Mode:** Blocks communication between specific segments.
* **Configuration Steps:**
  1. In Teams Admin Center, go to "Org-wide settings."
  2. Select "Information barriers."
  3. Choose the barrier mode (Allow List or Block List).
  4. Configure segment associations for users or groups.
  5. Save and apply settings.

**Configuring SharePoint for IBs:**

* **Barrier Modes:** SharePoint supports two barrier modes for IB enforcement:
  1. **Limited Access Mode:** Provides read-only access to specified segments.
  2. **Full Access Mode:** Allows collaboration and editing within specified segments.
* **Configuration Steps:**
  1. In SharePoint Admin Center, go to "Policies and compliance."
  2. Select "Information barriers."
  3. Choose the barrier mode (Limited Access or Full Access).
  4. Configure segment associations for SharePoint sites, libraries, or items.
  5. Save and apply settings.

**Configuring OneDrive for IBs:**

* **Barrier Modes:** OneDrive supports barrier modes similar to SharePoint.
  1. **Limited Access Mode:** Provides read-only access to specific segments.
  2. **Full Access Mode:** Allows collaboration and editing within specified segments.
* **Configuration Steps:**
  1. In OneDrive Admin Center, go to "Policies and compliance."
  2. Select "Information barriers."
  3. Choose the barrier mode (Limited Access or Full Access).
  4. Configure segment associations for OneDrive accounts or folders.
  5. Save and apply settings.

**Best Practices:**

* Clearly define barrier mode requirements based on compliance needs.
* Regularly review and update segment associations for accuracy.
* Test IB configurations to ensure they align with organizational policies.

### Investigate issues with IB policies

**Investigating IB Policy Issues:**

* **Definition:** Investigating issues with Information Barriers (IB) policies in Microsoft Purview involves identifying and resolving problems related to communication and data sharing restrictions between segments.

**Troubleshooting Steps:**

1. **Identify the Issue:**
   * Determine the specific nature of the problem, such as blocked communication or unauthorized access.
2. **Review Policy Configuration:**
   * Examine the IB policy settings to ensure they align with organizational requirements.
   * Check conditions, actions, and segment associations.
3. **Check Segment Membership:**
   * Verify that users and groups are correctly assigned to the appropriate segments.
   * Ensure segments are up-to-date with current membership.
4. **Examine User Attributes:**
   * Confirm that user attributes (e.g., department, job role) are accurate and consistent with policy conditions.
5. **Logs and Notifications:**
   * Review IB logs and notifications to identify policy violations or events.
   * Investigate any alerts or notifications related to IB issues.
6. **Testing and Validation:**
   * Test policy enforcement in a controlled environment to replicate the issue.
   * Validate whether the policy is blocking or allowing communication as intended.
7. **Communication and User Feedback:**
   * Communicate with affected users to gather additional information about the issue.
   * Collect feedback and user experiences to aid in troubleshooting.
8. **Documentation and Reporting:**
   * Document the issue, steps taken for investigation, and any findings.
   * Create incident reports if needed for tracking and resolution.
9. **Escalation:**
   * If the issue cannot be resolved at your level, escalate it to higher-level support or Microsoft support if necessary.

**Common Issues and Solutions:**

* **Misconfigured Policies:** Review and adjust policy conditions, actions, and associations.
* **Incorrect Segment Membership:** Verify user and group membership in segments.
* **Outdated User Attributes:** Ensure user attributes are accurate and up-to-date.
* **Logs and Notifications:** Investigate logs for specific policy violations.
* **Testing:** Use test accounts and scenarios to validate policy behavior.

**Best Practices:**

* Keep accurate documentation of IB policy configurations and investigations.
* Maintain open communication with affected users for quick issue resolution.
* Periodically review and audit IB policies to ensure ongoing compliance.

## Implement and manage privacy requirements by using Microsoft Priva

### Configure and maintain privacy risk management

**Privacy Risk Management:**

* **Definition:** Privacy Risk Management in Microsoft Purview involves setting up and maintaining processes to identify, assess, and mitigate privacy risks associated with data handling and compliance.

**Configuration Steps:**

1. **Data Classification:**
   * Classify data according to sensitivity and privacy requirements using labels or tags.
2. **Privacy Compliance Settings:**
   * Configure privacy compliance settings in Purview to align with regulatory standards (e.g., GDPR, HIPAA).
3. **Data Discovery:**
   * Implement data discovery tools to locate and identify sensitive data across your organization.
4. **Data Protection:**
   * Apply encryption, access controls, and rights management to protect sensitive data.
5. **Auditing and Monitoring:**
   * Set up auditing and monitoring to track data access and changes, ensuring compliance.
6. **User Training and Awareness:**
   * Educate employees about privacy policies, data handling, and their role in compliance.

**Maintaining Privacy Risk Management:**

* **Regular Assessments:** Continuously assess and update privacy risk assessments.
* **Policy Review:** Periodically review and update privacy policies to align with changing regulations and organizational needs.
* **Incident Response:** Develop and maintain an incident response plan for data breaches or privacy incidents.
* **Monitoring Tools:** Use automated monitoring tools to keep track of data handling activities and privacy risks.
* **Compliance Audits:** Conduct regular compliance audits to ensure adherence to privacy regulations.

**Best Practices:**

* Stay informed about privacy regulations and compliance requirements relevant to your organization.
* Foster a culture of privacy awareness and responsibility among employees.
* Collaborate with legal and compliance teams to ensure alignment with regulatory standards.
* Establish a dedicated privacy team or officer to oversee privacy risk management.

### Create and manage Privacy Risk Management policies

* **Definition:** Privacy Risk Management policies in Microsoft Purview are a set of rules and guidelines that govern how an organization identifies, assesses, and mitigates privacy risks associated with data handling and compliance.

**Creating Privacy Risk Management Policies:**

1. **Policy Objectives:**
   * Define the objectives and scope of the policy. What privacy risks are you addressing? What regulations or standards apply?
2. **Data Classification:**
   * Specify data classification criteria, such as sensitive, confidential, or public data.
3. **Privacy Controls:**
   * Define the privacy controls and measures to protect sensitive data, including encryption, access controls, and data retention policies.
4. **Data Handling Procedures:**
   * Document procedures for collecting, storing, and sharing data in compliance with privacy regulations.
5. **Data Breach Response:**
   * Outline steps for detecting, reporting, and mitigating data breaches. Include incident response protocols.
6. **User Training and Awareness:**
   * Describe training requirements and awareness programs to educate employees on privacy policies.

**Managing Privacy Risk Management Policies:**

* **Regular Review:** Periodically review and update policies to align with changing regulations and organizational needs.
* **Compliance Audits:** Conduct audits to ensure policies are being followed and are in compliance with privacy regulations.
* **Incident Reporting:** Establish a reporting mechanism for employees to report privacy incidents or breaches.
* **Documentation:** Maintain detailed records of policy changes, audits, and incidents for accountability and compliance purposes.

**Best Practices:**

* Collaborate with legal and compliance teams to ensure policies align with regulatory standards.
* Train employees on policy changes and privacy best practices regularly.
* Implement automated tools for data classification and monitoring to enforce policy compliance.
* Engage a dedicated privacy officer or team to oversee policy creation and enforcement.

### Identify and monitor potential risks involving personal data

**Identifying Risks:**

* **Data Inventory:** Create an inventory of personal data across your organization, including its sources, storage locations, and usage.
* **Data Classification:** Classify data based on sensitivity and privacy requirements to identify areas with higher risk.
* **Data Mapping:** Map data flows to understand how personal data moves within and outside the organization.
* **Privacy Impact Assessments (PIAs):** Conduct PIAs to assess the impact of data processing activities on privacy and identify potential risks.

**Monitoring Risks:**

* **Data Auditing:** Implement data auditing and logging to track access, changes, and sharing of personal data.
* **Anomaly Detection:** Use AI and machine learning tools to identify unusual data access patterns or behaviors that may indicate a breach or misuse.
* **Incident Response Plans:** Develop and maintain incident response plans to address potential risks promptly.
* **Regular Assessments:** Continuously assess privacy risks and vulnerabilities, especially when new data processing activities are introduced.

**Compliance Tools:**

* **Microsoft Purview Compliance Center:** Utilize Purview Compliance Center to monitor and manage compliance with data protection regulations.
* **Data Loss Prevention (DLP):** Implement DLP policies to prevent the unauthorized sharing of personal data.
* **Threat Protection:** Use threat protection solutions to detect and respond to potential data breaches.

**Best Practices:**

* Keep up-to-date with data protection regulations relevant to your industry and geography.
* Establish a dedicated privacy team or officer responsible for risk identification and monitoring.
* Conduct regular privacy risk assessments to proactively address potential issues.
* Train employees to recognize and report privacy risks and incidents.

### Evaluate and remediate alerts and issues

**Alert and Issue Evaluation:**

* **Alert Sources:** Alerts and issues in Microsoft Purview can come from various sources, including compliance policies, security monitoring, and data governance.
* **Severity Assessment:** Evaluate the severity of each alert or issue to prioritize remediation efforts.
* **Root Cause Analysis:** Investigate the root causes of alerts to understand the underlying problems.
* **Data Analysis:** Examine relevant data, logs, and audit trails to gather evidence and context.

**Remediation Steps:**

1. **Incident Triage:**
   * Determine the nature of the alert and its potential impact on data security or compliance.
2. **Isolation:** If necessary, isolate affected systems or data to prevent further harm.
3. **Alert Resolution:**
   * Address the specific issue that triggered the alert, following established procedures and best practices.
4. **Documentation:**
   * Document the remediation process, including actions taken, findings, and outcomes.
5. **Notification:** Notify relevant stakeholders, such as compliance officers or security teams, about the alert and remediation progress.
6. **Monitoring:** Implement continuous monitoring to ensure that the issue does not reoccur.

**Best Practices:**

* Establish incident response plans and workflows for different types of alerts and issues.
* Collaborate with cross-functional teams, including IT, compliance, and security, to ensure effective remediation.
* Conduct post-incident reviews to identify areas for improvement and prevent future occurrences.
* Automate alert handling and remediation where possible to expedite response times.

### Implement and manage subject rights requests

**Subject Rights Requests (SRRs):**

* **Definition:** Subject Rights Requests in Microsoft Purview refer to requests made by individuals (data subjects) to exercise their rights under data protection regulations, such as GDPR or CCPA.

**Implementing SRRs:**

1. **Data Collection and Storage:** Ensure you have a centralized repository of personal data and records of data subjects' consent and preferences.
2. **Request Channels:** Establish clear channels through which data subjects can submit SRRs, such as email or a designated portal.
3. **Identity Verification:** Implement a robust process for verifying the identity of data subjects to prevent fraudulent requests.
4. **Response Time:** Comply with regulatory requirements by acknowledging SRRs promptly and responding within the specified time frame (e.g., 30 days under GDPR).
5. **Data Access:** Provide data subjects with access to their personal data stored in Purview, allowing them to review, download, or request copies.
6. **Data Deletion:** Enable data subjects to request the deletion of their personal data, including data held by third parties or data processing partners.

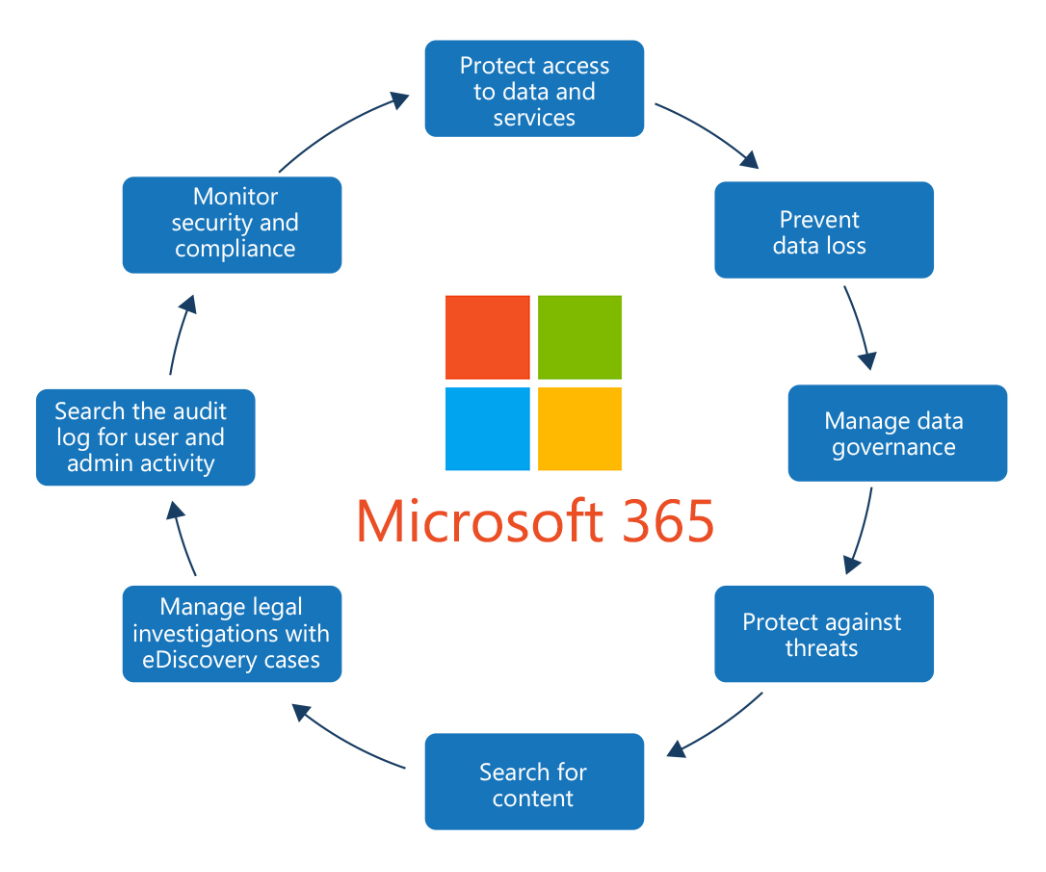
**Managing SRRs:**

* **SRR Tracking:** Maintain a systematic record of all SRRs, including details of the request, verification, response, and any actions taken.
* **Privacy Dashboard:** Leverage Microsoft Purview's privacy management tools and dashboards to track and manage SRRs efficiently.
* **Communication:** Maintain open and transparent communication with data subjects throughout the SRR process, providing updates on the status of their requests.
* **Data Portability:** Support data subjects in transferring their data to other organizations as required by data protection regulations.

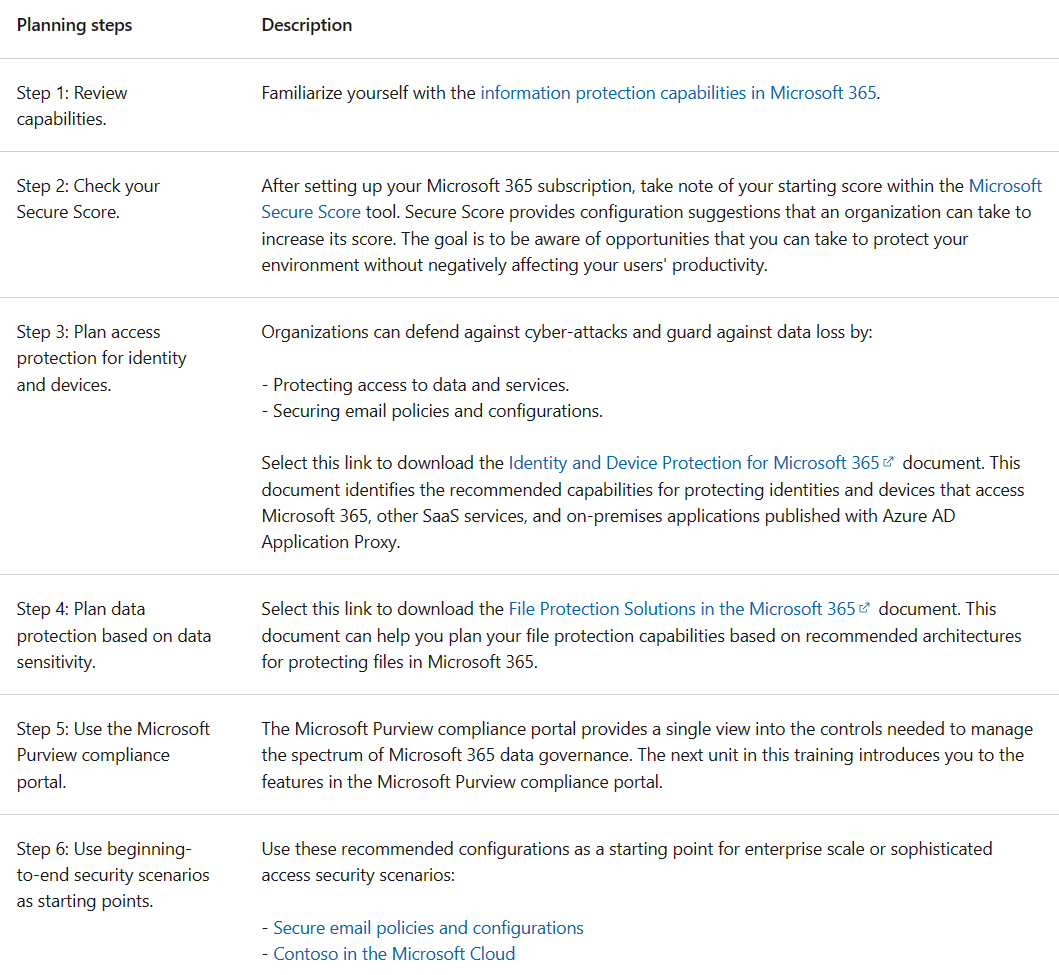
**Best Practices:**

* Train personnel responsible for handling SRRs on data protection regulations and Purview's tools.
* Develop and document clear procedures for SRR handling, including escalation processes for complex requests.
* Regularly audit and review SRR processes to ensure compliance with changing regulations.
* Collaborate with legal and compliance teams to align SRR processes with legal requirements.

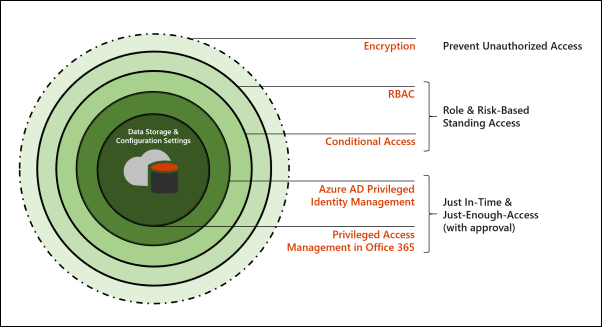
# Diagrams & Notes



### Plan for security and compliance in Microsoft 365



### Layers of Protection



### Privileged access management architecture & approval workflow

1. Configure privileged access policy



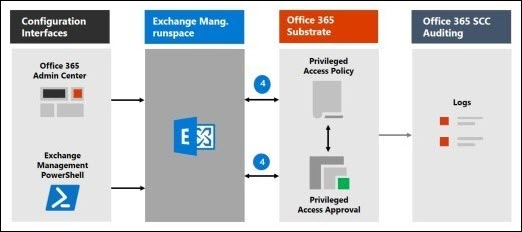
2. Access Request



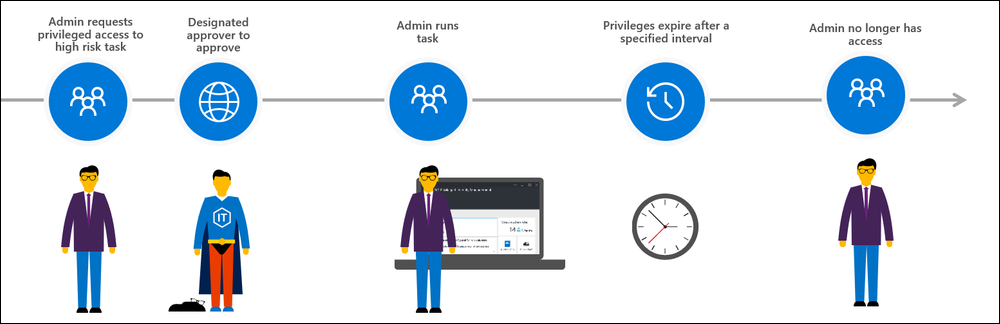
3. Access approval



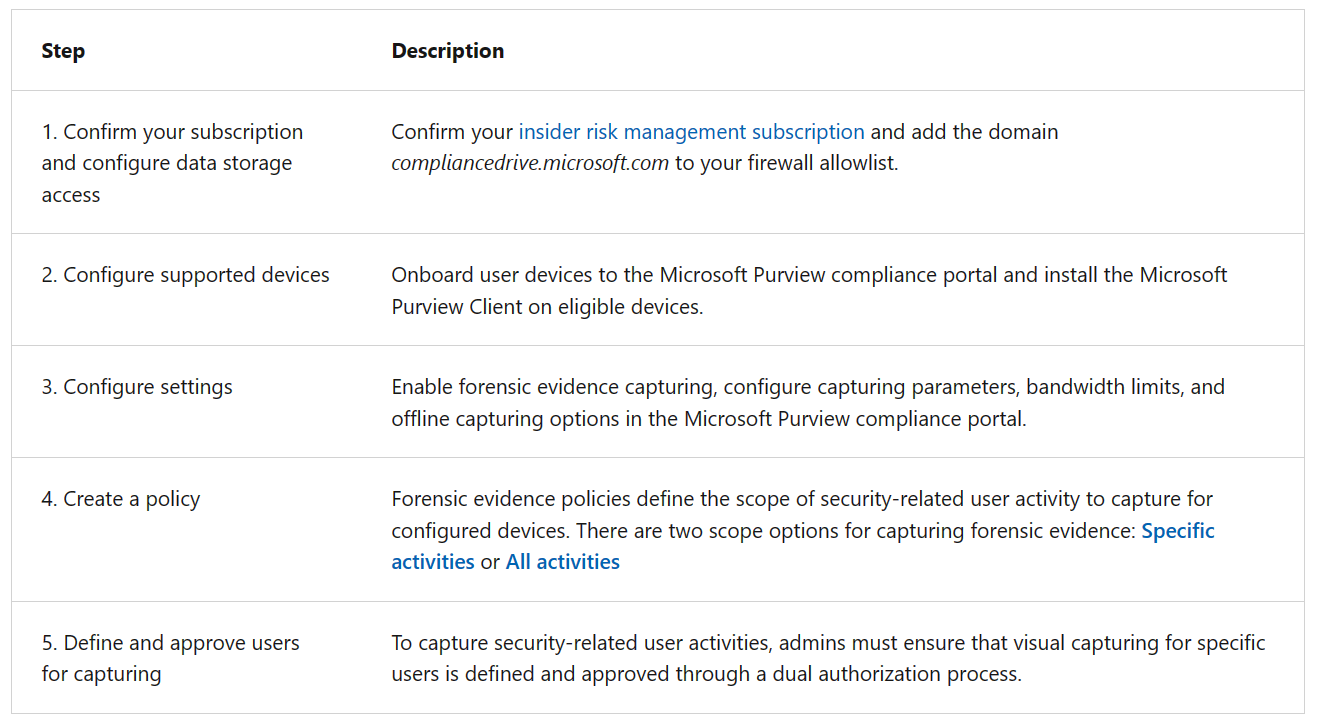
4. Access processing



### Approval Workflow



### Configure Forensic Evidence in 365



### Configure Approved users for Forensic Evidence Capturing

1. In the [Microsoft Purview compliance portal](https://compliance.microsoft.com/), go to **Insider risk management** > **Forensic evidence** > **User management**.
2. Select the **Manage forensic evidence requests** tab.
3. Select **Create request**.
4. On the **Users** page, select **Add users**.
5. Use **Search** to locate a specific user or select one or more users from the list. Select **Add**, then select **Next**.
6. On the **Forensic evidence policy** page, select a forensic evidence policy for the added users. The policy you choose determines the scope of activity to capture for users. Select **Next**.
7. On the **Justification** page, let the reviewer know why you're requesting that capturing be enabled for the users you added in the **Justification for turning on forensic evidence capturing** text box. This field is required. When complete, select **Next**.
8. On the **Email notifications** page, use a template to notify users that forensic evidence capturing is enabled on their devices, following your organization's policies. Emails are sent only if requests are approved.

Select the **Send an email notification to approved users** check box. Choose an existing template or create a new template by selecting **Create a notification template**.

1. On the **Finish** page, review your settings before submitting the request. Select **Edit users** or **Edit justification** to change any of the request values or select **Submit** to create and send the request to reviewers.

### 

### 

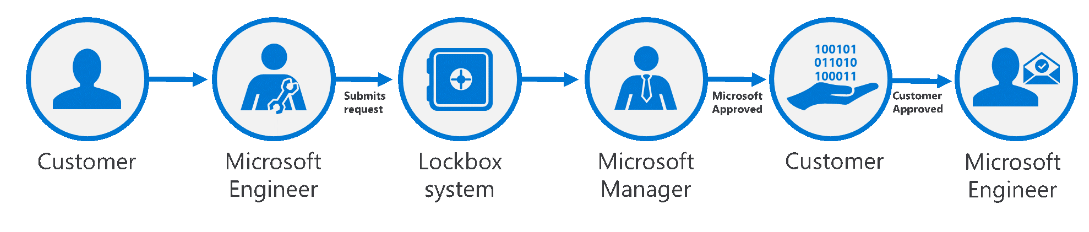
### Customer Lockbox workflow

1. After you troubleshoot the issue but can't fix it, you open a support request with Microsoft Support.
2. A Microsoft engineer reviews the service request and determines a need to access the organization's tenant to repair the issue in Exchange Online.
3. The Microsoft engineer logs into the Customer Lockbox request tool and makes a data access request that includes the organization's tenant name, service request number, and the estimated time the engineer needs access to the data.
4. After a Microsoft Support manager approves the request, Customer Lockbox sends the designated approver at the organization an email notification about the pending access request from Microsoft. Anyone with a work or school account who has been granted the global administrator role or someone assigned the Customer Lockbox access approver admin role in Microsoft 365 admin center can approve Customer Lockbox requests.

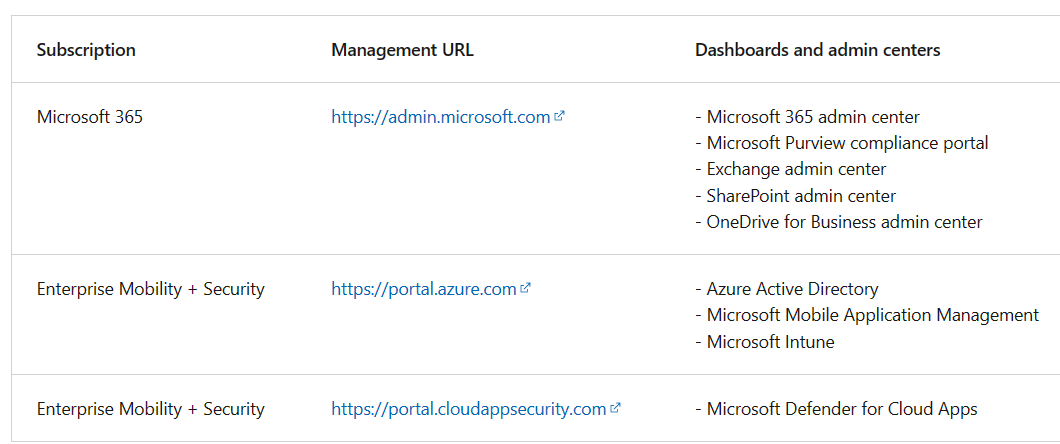
Customer Lockbox requests have a default duration of 12 hours. If you don't respond to a request within 12 hours, the request expires.

1. The approver signs into the Microsoft 365 admin center and approves the request. This step triggers the creation of an audit record available by searching the audit log. All actions performed by a Microsoft engineer are logged in the audit log. You can search for and review these audit records. Before you can use the audit log to track requests for Customer Lockbox, there are some steps you need to take to set up audit logging. For more information, see Search the audit log in the [Microsoft 365 Defender portal](https://learn.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#before-you-begin?azure-portal=true).
2. After the approver from the organization approves the request, the Microsoft engineer receives the approval message, logs into the tenant in Exchange Online, and fixes the customer's issue.

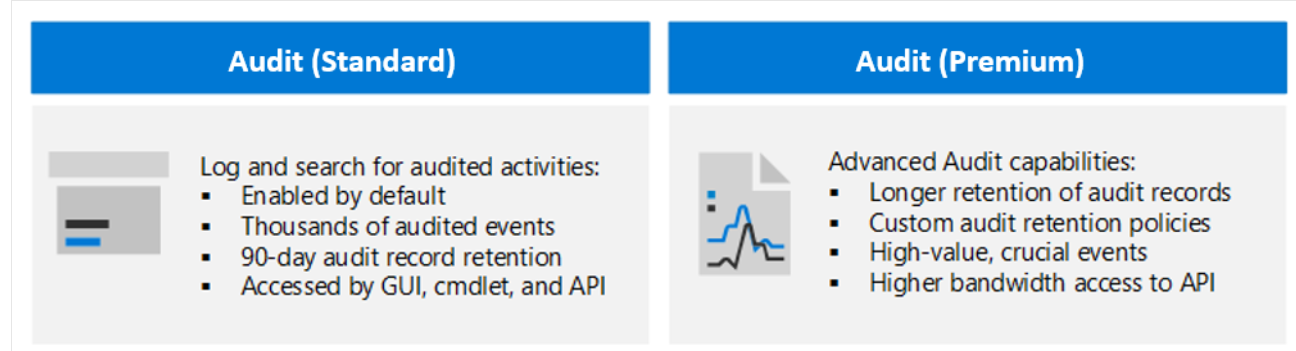
Currently, the maximum period for the access permissions granted to the Microsoft engineer is 4 hours. The Microsoft engineer can also request a shorter period.

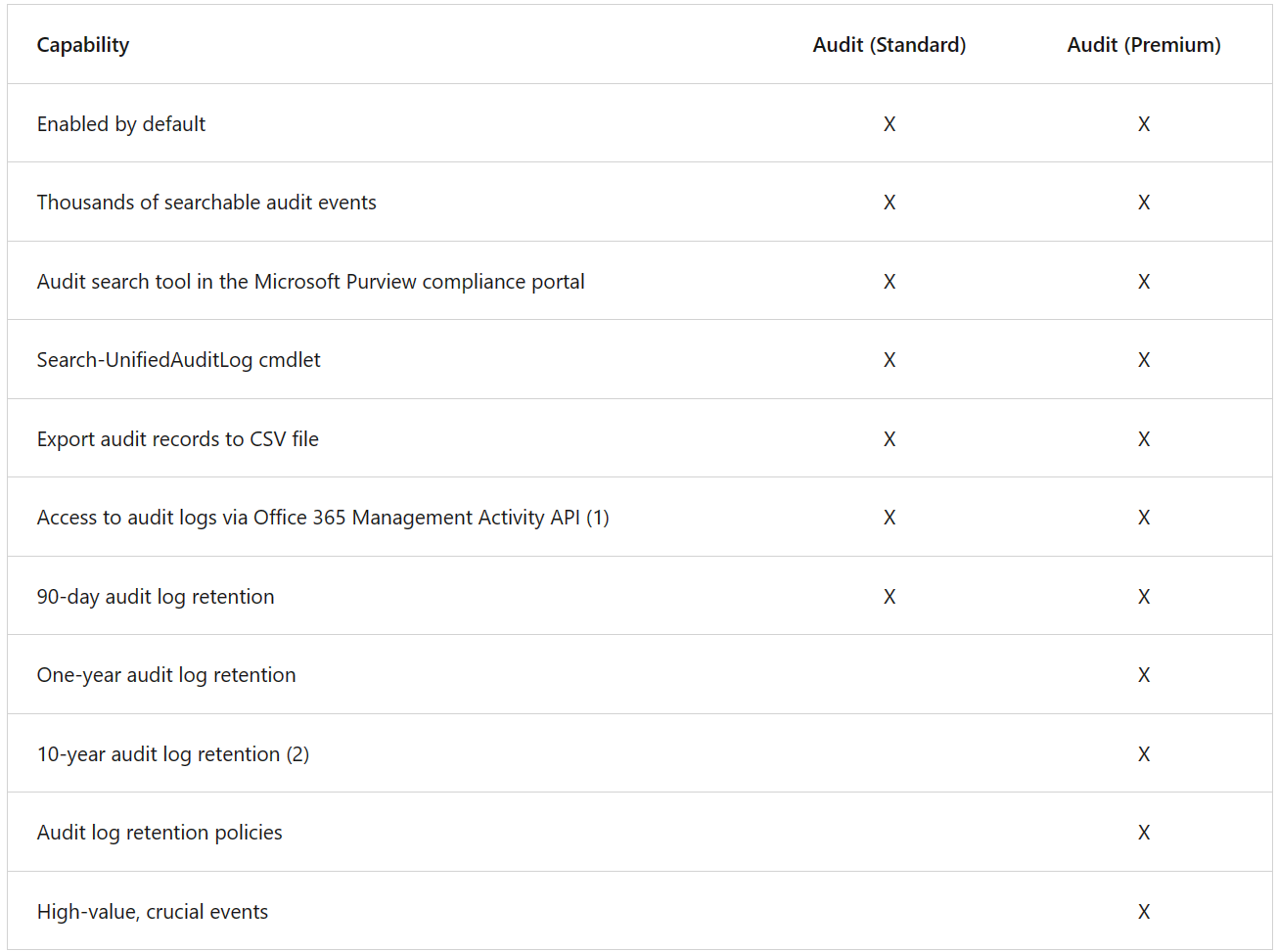


### 3 Big MS Portals

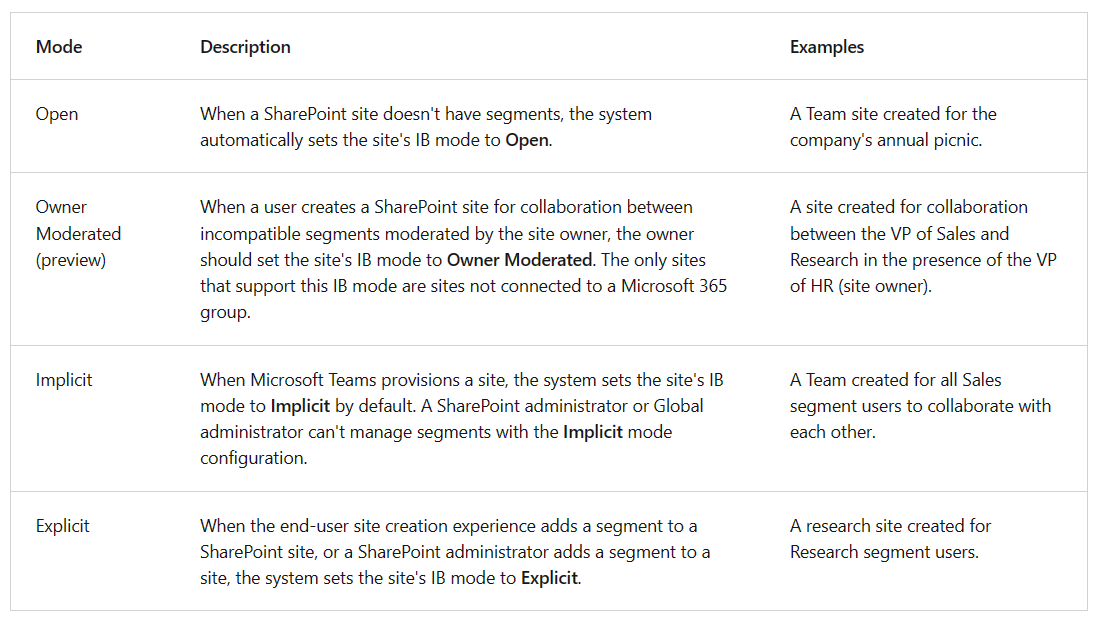


### MS Purview Audit Standard vs Premium

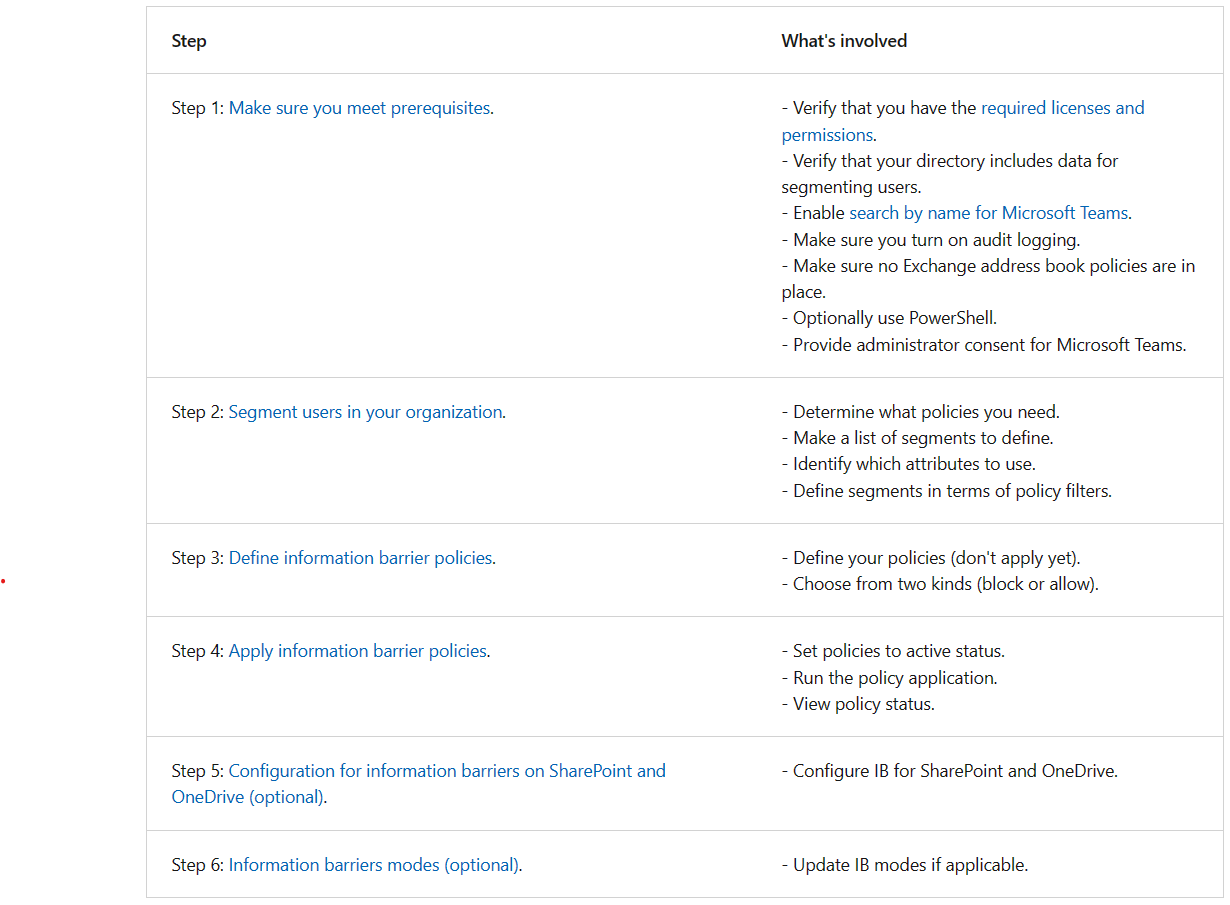




### Understanding Information barrier types



### Configure information barriers for Microsoft 365



### Enable SharePoint & OneDrive Info Barriers in a org

1. [Download](https://www.microsoft.com/download/details.aspx?id=35588) and install the latest version of SharePoint Online Management Shell.
2. Connect to SharePoint Online as a global admin or SharePoint admin in Microsoft 365.
3. To enable information barriers in SharePoint and OneDrive, run the following command:

**PowerShellCopy**

Set-SPOTenant -InformationBarriersSuspension $false

1. After you've enabled information barriers for SharePoint and OneDrive in your organization, wait for approximately 1 hour for the changes to take effect.

If you've enabled information barriers for SharePoint in your organization before March 15, 2022, the default access and sharing control for Implicit mode for Microsoft Teams-connected sites are based on the segments associated with the site.

To enable Microsoft 365 group-membership based access and sharing control for all Implicit mode Teams-connected sites in your tenant, run the following command:

**PowerShellCopy**

Set-SPOTenant -IBImplicitGroupBased $true

If you have Microsoft 365 Multi-Geo, you must run this command for each of your geo-locations.

To update a OneDrive site IB mode to **Owner Moderated**, run the following PowerShell command:

**PowerShellCopy**

Set-SPOSite -Identity <siteurl> InformationBarriersMode OwnerModerated

To view the IB mode of a OneDrive site, run the following command in the SharePoint Online Management Shell as a SharePoint admin or global administrator:

**PowerShellCopy**

Get-SPOSite -Identity <site URL> | Select InformationBarriersMode

For example:

**PowerShellCopy**

Get-SPOSite -Identity https://contoso-my.sharepoint.com/personal/John\_contoso\_onmicrosoft\_com | Select InformationBarriersMode

### Manage segments on a user’s OneDrive

To associate a segment with a OneDrive, run the following command in the SharePoint Online Management Shell. A OneDrive can have up to 100 associated segments.

**PowerShellCopy**

Set-SPOSite -Identity <site URL> -AddInformationSegment <segment GUID>

For example:

**PowerShellCopy**

Set-SPOSite -Identity https://contoso-my.sharepoint.com/personal/John\_contoso\_onmicrosoft\_com -AddInformationSegment 27d20a85-1c1b-4af2-bf45-a41093b5d111

When you add segments to a OneDrive, the system automatically sets the site's IB mode to **Explicit**. An error appears if you attempt to associate a segment that isn't compatible with the existing segments on the OneDrive.

To remove segment from a OneDrive, run the following command.

**PowerShellCopy**

Set-SPOSite -Identity <site URL> -RemoveInformationSegment <segment GUID>

For example:

**PowerShellCopy**

Set-SPOSite -Identity https://contoso-my.sharepoint.com/personal/John\_contoso\_onmicrosoft\_com -RemoveInformationSegment 27d20a85-1c1b-4af2-bf45-a41093b5d111

If an administrator removes all the segments of a OneDrive site, the system automatically sets the IB mode of the OneDrive site to **Open**.

### View the segments associated with OneDrive

1. Connect to the [Security & Compliance Center PowerShell](https://learn.microsoft.com/en-us/powershell/exchange/office-365-scc/connect-to-scc-powershell/connect-to-scc-powershell) as a Microsoft 365 Global administrator.
2. Run the following command to get the list of segments and their GUIDs.

**PowerShellCopy**

Get-OrganizationSegment | ft Name, EXOSegmentID

1. Save the list of segments. The following table identifies the segments for the Contoso scenario that this training unit presented earlier.

| **Name** | **EXOSegmentId** |
| --- | --- |
| Sales | a9592060-c856-4301-b60f-bf9a04990d4d |
| Research | 27d20a85-1c1b-4af2-bf45-a41093b5d111 |
| HR | a17efb47-e3c9-4d85-a188-1cd59c83de32 |

1. If not previously completed, download and install the latest SharePoint Online Management Shell. If you installed a previous version of the SharePoint Online Management Shell, follow the instructions in the [Enable SharePoint and OneDrive information barriers in your organization](https://learn.microsoft.com/en-us/sharepoint/information-barriers#enable-sharepoint-and-onedrive-information-barriers-in-your-organization?azure-portal=true) article.
2. Connect to SharePoint as a global admin or SharePoint admin in Microsoft 365.
3. Run the following command:

**PowerShellCopy**

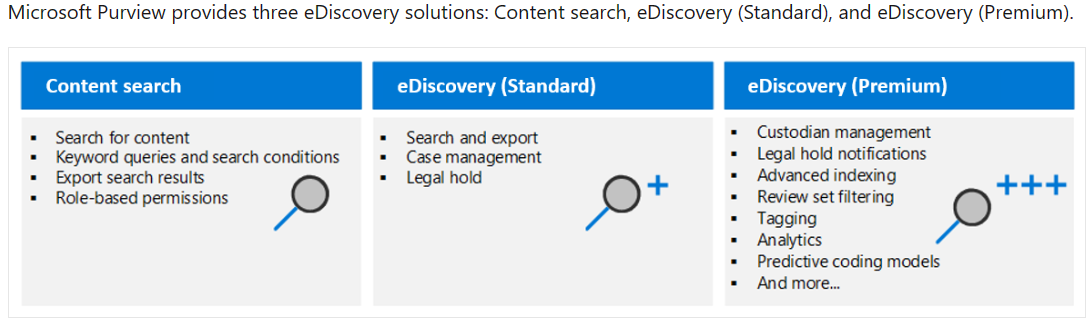
Get-SPOSite -Identity <site URL> | Select InformationSegment

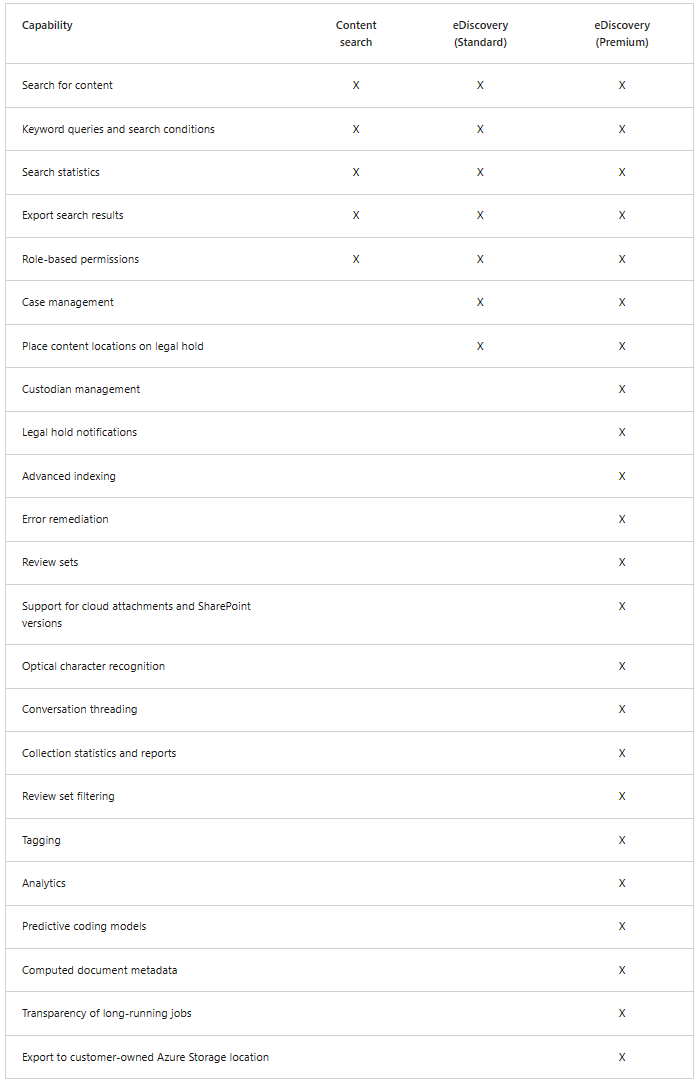
For example:

**PowerShellCopy**

Get-SPOSite -Identity https://contoso-my.sharepoint.com/personal/John\_contoso\_onmicrosoft\_com | Select Info

### eDiscover Solutions





### Microsoft Purview Permission Examples

This section provides examples of using the **New-ComplianceSecurityFilter** cmdlet to create a search permissions filter.

This example allows members of the "US Discovery Managers" role group to search only the mailboxes and OneDrive accounts in the United States.

**PowerShellCopy**

New-ComplianceSecurityFilter -FilterName USDiscoveryManagers -Users "US Discovery Managers" -Filters "Mailbox\_CountryOrRegion -eq 'United States'"

This example allows the user "annb@contoso.com" to perform search actions only for mailboxes and OneDrive accounts in Canada. This filter contains the three-digit numeric country code for Canada from ISO 3166-1.

**PowerShellCopy**

New-ComplianceSecurityFilter -FilterName CountryFilter -Users annb@contoso.com -Filters "Mailbox\_CountryCode -eq '124'"

This example allows the users "donh" and "suzanf" to search only the mailboxes and OneDrive accounts that have the value 'Marketing' for the CustomAttribute1 mailbox property.

**PowerShellCopy**

New-ComplianceSecurityFilter -FilterName MarketingFilter -Users donh,suzanf -Filters "Mailbox\_CustomAttribute1 -eq 'Marketing'"

This example allows members of the "Fourth Coffee eDiscovery Managers" role group to search only the mailboxes and OneDrive accounts that have the value 'FourthCoffee' for the Department mailbox property. The filter also allows the role group members to search for documents in the Fourth Coffee SharePoint site.

**PowerShellCopy**

New-ComplianceSecurityFilter -FilterName "Fourth Coffee Security Filter" -Users "Fourth Coffee eDiscovery Managers", "Fourth Coffee Investigators" -Filters "Mailbox\_Department -eq 'FourthCoffee'", "SiteContent\_Path -like 'https://contoso.sharepoint.com/sites/FourthCoffee' -or SiteContent\_Path -like 'https://contoso-my.sharepoint.com/personal'"

**Note**

In the previous example, an extra site content filter (SiteContent\_Path -like 'https://contoso-my.sharepoint.com/personal') has to be included so that role group members can search for documents in OneDrive accounts. If this filter isn't included, the filter would only allow role group members to search for documents located in [**https://contoso.sharepoint.com/sites/FourthCoffee**](https://contoso.sharepoint.com/sites/FourthCoffee).

This example allows members of the eDiscovery Manager role group to search only the mailboxes and OneDrive accounts of members of the Ottawa Users distribution group. The Get-DistributionGroup cmdlet in Exchange Online PowerShell is used to find the members of the Ottawa Users group.

**PowerShellCopy**

$DG = Get-DistributionGroup "Ottawa Users"

PowerShellCopy

New-ComplianceSecurityFilter -FilterName DGFilter -Users eDiscoveryManager -Filters "Mailbox\_MemberOfGroup -eq '$($DG.DistinguishedName)'"

This example prevents any user from performing search actions on the mailboxes and OneDrive accounts of members of the Executive Team distribution group. That means users can delete content from these mailboxes. The Get-DistributionGroup cmdlet in Exchange Online PowerShell is used to find the members of the Executive Team group.

**PowerShellCopy**

$DG = Get-DistributionGroup "Executive Team"

**PowerShellCopy**

New-ComplianceSecurityFilter -FilterName NoExecutivesPreview -Users All -Filters "Mailbox\_MemberOfGroup -ne '$($DG.DistinguishedName)'"

This example allows members of the OneDrive eDiscovery Managers custom role group to only search for content in OneDrive accounts in the organization.

**PowerShellCopy**

New-ComplianceSecurityFilter -FilterName OneDriveOnly -Users "OneDrive eDiscovery Managers" -Filters "SiteContent\_Path -like 'https://contoso-my.sharepoint.com/personal'"

This example restricts the user to performing search actions only on email messages sent during the calendar year 2020.

**PowerShellCopy**

New-ComplianceSecurityFilter -FilterName EmailDateRestrictionFilter -Users donh@contoso.com -Filters "MailboxContent\_Received -ge '01-01-2020' -and MailboxContent\_Received -le '12-31-2020'"

Similar to the previous example, this example restricts the user to performing search actions only on documents that were last changed sometime in the calendar year 2020.

**PowerShellCopy**

New-ComplianceSecurityFilter -FilterName DocumentDateRestrictionFilter -Users donh@contoso.com -Filters "SiteContent\_LastModifiedTime -ge '01-01-2020' -and SiteContent\_LastModifiedTime -le '12-31-2020'"

This example prevents members of the "OneDrive Discovery Managers" role group from performing search actions on any mailbox in the organization.

**PowerShellCopy**

New-ComplianceSecurityFilter -FilterName NoEXO -Users "OneDrive Discovery Managers" -Filters "Mailbox\_Alias -notlike '\*'"

This example prevents anyone in the organization from performing search actions on email messages that were sent or received by "janets" or "sarad".

**PowerShellCopy**

New-ComplianceSecurityFilter -FilterName NoSaraJanet -Users All -Filters "MailboxContent\_Participants -notlike 'janets@contoso.onmicrosoft.com' -and MailboxContent\_Participants -notlike 'sarad@contoso.onmicrosoft.com'"

This example uses a filters list to combine mailbox and site filters. In this example, the mailbox filter is a content location filter and the site filter is a content filter.

**PowerShellCopy**

New-ComplianceSecurityFilter -FilterName "Coho Winery Security Filter" -Users "Coho Winery eDiscovery Managers"

### Audit Logs to Investigate Common Issue’s

[Use audit log searching to investigate common support issues - Training | Microsoft Learn](https://learn.microsoft.com/en-us/training/modules/manage-microsoft-purview-audit-standard/6-use-audit-log-searching-investigate-common-support-issues)

### Additional Resources

[Microsoft Purview | Microsoft Learn](https://learn.microsoft.com/en-us/purview/)

[Auditing solutions in Microsoft Purview | Microsoft Learn](https://learn.microsoft.com/en-us/purview/audit-solutions-overview)