SC-400 Study Notes

[Implement information protection (25–30%) 2](#_Toc145325217)

[Create and manage sensitive info types 2](#_Toc145325218)

[Create and manage trainable classifiers 6](#_Toc145325219)

[Implement and manage sensitivity labels 9](#_Toc145325220)

[Design and implement encryption for email messages 13](#_Toc145325221)

[Implement DLP (15–20%) 15](#_Toc145325222)

# 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.

As a Microsoft Trainer helping prepare for the SC-400 exam. Provide study notes as brief as possible on the following topic “Remediate DLP alerts generated by Defender for Cloud Apps”.

**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
* Create retention labels for data lifecycle management
* Configure and manage adaptive scopes
* Configure a retention label policy to publish labels
* Configure a retention label policy to auto-apply labels
* Interpret the results of policy precedence, including using Policy lookup

**Manage data retention in Microsoft 365 workloads**

* Create and apply retention policies for SharePoint and OneDrive
* Create and apply retention policies for Microsoft 365 groups
* Create and apply retention policies for Teams
* Create and apply retention policies for Yammer
* Create and apply retention policies for Exchange Online
* Apply mailbox holds in Exchange Online
* Implement Exchange Online archiving policies
* Configure preservation locks for retention policies and retention label policies
* Recover retained content in Microsoft 365

**Implement Microsoft Purview records management**

* Create and configure retention labels for records management
* Manage retention labels by using a file plan, including file plan descriptors
* Classify records by using retention labels and retention label policies
* Manage event-based retention
* Manage the disposition of content in records management
* Configure records management settings, including retention label settings and disposition settings

**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
* Create and manage assessments
* Create and modify custom templates
* Interpret and manage improvement actions
* Create and manage alert policies for assessments

**Plan and manage eDiscovery and Content search**

* Choose between eDiscovery (Standard) and eDiscovery (Premium) based on an organization’s requirements
* Plan and implement eDiscovery
* Delegate permissions to use eDiscovery and Content search
* Perform searches and respond to results from eDiscovery
* Manage eDiscovery cases
* Perform searches by using Content search

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

* Choose between Audit (Standard) and Audit (Premium) based on an organization’s requirements
* Plan for and configure auditing
* Investigate activities by using the unified audit log
* Review and interpret compliance reports and dashboards
* Configure alert policies
* Configure audit retention policies

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

**Implement and manage Microsoft Purview Communication Compliance**

* Plan for communication compliance
* Create and manage communication compliance policies
* Investigate and remediate communication compliance alerts and reports

**Implement and manage Microsoft Purview Insider Risk Management**

* Plan for insider risk management
* Create and manage insider risk management policies
* Investigate and remediate insider risk activities, alerts, and reports
* Manage insider risk cases
* Manage forensic evidence settings
* Manage notice templates

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

* Plan for IBs
* Create and manage IB segments and policies
* Configure Teams, SharePoint, and OneDrive to enforce IBs, including setting barrier modes
* Investigate issues with IB policies

**Implement and manage privacy requirements by using Microsoft Priva**

* Configure and maintain privacy risk management
* Create and manage Privacy Risk Management policies
* Identify and monitor potential risks involving personal data
* Evaluate and remediate alerts and issues
* Implement and manage subject rights requests