SC-401: Microsoft Certified: Information Security Administrator Associate

Course Outline

Note: The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. Related topics may be covered in the exam

Skills at a glance

- Implement information protection (30–35%)
- Implement data loss prevention and retention (30–35%)
- Manage risks, alerts, and activities (30–35%)

Implement information protection (30–35%)

Implement and manage data classification

- Identify sensitive information requirements for an organization's data
- Translate sensitive information requirements into built-in or custom sensitive info types
- Create and manage custom sensitive info types
- Implement document fingerprinting
- Create and manage exact data match (EDM) classifiers
- Create and manage trainable classifiers
- Monitor data classification and label usage by using data explorer and content explorer
- Configure optical character recognition (OCR) support for sensitive info types

Implement and manage sensitivity labels in Microsoft Purview

- Implement roles and permissions for administering sensitivity labels
- Define and create sensitivity labels for items and containers

- Configure protection settings and content marking for sensitivity labels
- Configure and manage publishing policies for sensitivity labels
- Configure and manage auto-labeling policies for sensitivity labels
- Apply a sensitivity label to containers, such as Microsoft Teams, Microsoft 365 Groups, Microsoft Power BI, and Microsoft SharePoint
- Apply sensitivity labels by using Microsoft Defender for Cloud Apps

Implement information protection for Windows, file shares, and Exchange

- Plan and implement the Microsoft Purview Information Protection client
- Manage files by using the Microsoft Purview Information Protection client
- Apply bulk classification to on-premises data by using the Microsoft Purview Information Protection scanner
- Design and implement Microsoft Purview Message Encryption
- Design and implement Microsoft Purview Advanced Message Encryption

Implement data loss prevention and retention (30–35%)

Create and configure data loss prevention policies

- Design data loss prevention policies based on an organization's requirements
- Implement roles and permissions for data loss prevention
- Create and manage data loss prevention policies
- Configure data loss prevention policies for Adaptive Protection
- Interpret policy and rule precedence in data loss prevention
- Create file policies in Microsoft Defender for Cloud Apps by using a DLP policy

Implement and monitor Microsoft Purview Endpoint DLP

- Specify device requirements for Endpoint DLP, including extensions
- Configure advanced DLP rules for devices in DLP policies
- Configure Endpoint DLP settings
- Configure just-in-time protection
- Monitor endpoint activities

Implement and manage retention

- Plan for information retention and disposition by using retention labels
- Create, configure, and manage adaptive scopes
- Create retention labels for data lifecycle management
- 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
- Create and configure retention policies
- Recover retained content in Microsoft 365

Manage risks, alerts, and activities (30–35%)

Implement and manage Microsoft Purview Insider Risk Management

- Implement roles and permissions for Insider Risk Management
- Plan and implement Insider Risk Management connectors
- Plan and implement integration with Microsoft Defender for Endpoint
- Configure and manage Insider Risk Management settings
- Configure policy indicators
- Select an appropriate policy template
- Create and manage Insider Risk Management policies

- Manage forensic evidence settings
- Enable and configure insider risk levels for Adaptive Protection
- Manage insider risk alerts and cases
- Manage Insider Risk Management workflow, including notice templates

Manage information security alerts and activities

- Assign Microsoft Purview Audit (Premium) user licenses
- Investigate activities by using Microsoft Purview Audit
- Configure audit retention policies
- Analyze Purview activities by using activity explorer
- Respond to data loss prevention alerts in the Microsoft Purview portal
- Investigate insider risk activities by using the Microsoft Purview portal
- Respond to Purview alerts in Microsoft Defender XDR
- Respond to Defender for Cloud Apps file policy alerts
- Perform searches by using Content search

Protect data used by AI services

- Implement controls in Microsoft Purview to protect content in an environment that uses AI services
- Implement controls in Microsoft 365 productivity workloads to protect content in an environment that uses AI services
- Implement pre-requisites for Data Security Posture Management (DSPM) for AI
- Manage roles and permissions for DSPM for AI
- Configure DSPM for AI policies
- Monitor activities in DSPM for AI