Exam SC-400: Microsoft Information Protection Administrator – Skills Measured

Audience Profile

The Information Protection Administrator plans and implements controls that meet organizational compliance needs. This person is responsible for translating requirements and compliance controls into technical implementation. They assist organizational control owners to become and stay compliant.

They work with information technology (IT) personnel, business application owners, human resources, and legal stakeholders to implement technology that supports policies and controls necessary to sufficiently address regulatory requirements for their organization. They also work with the compliance and security leadership such as a Chief Compliance Officer and Security Officer to evaluate the full breadth of associated enterprise risk and partner to develop those policies.

This person defines applicable requirements and tests IT processes and operations against those policies and controls. They are responsible for creating policies and rules for content classification, data loss prevention, governance, and protection.

Skills Measured

NOTE: The bullets that appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

NOTE: Most questions cover features that are General Availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Implement Information Protection (35-40%)

Create and manage sensitive information types

- select a sensitive information type based on an organization's requirements
- create and manage custom sensitive information types
- create custom sensitive information types with exact data match
- implement document fingerprinting
- create a keyword dictionary

Create and manage trainable classifiers

- identify when to use trainable classifiers
- create a trainable classifier
- verify a trainable classifier is performing properly
- retrain a classifier

Implement and manage sensitivity labels

- identify roles and permissions for administering sensitivity labels
- create sensitivity labels
- configure and manage sensitivity label policies
- apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites
- configure and publish automatic labeling policies (excluding MCAS scenarios)
- monitor label usage by using label analytics
- apply bulk classification to on-premises data by using the AIP unified labelling scanner
- manage protection settings and marking for applied sensitivity labels
- apply protections and restrictions to email including content marking, usage, permission, encryption, expiration, etc.
- apply protections and restrictions to files including content marking, usage, permission, encryption, expiration, etc.

Plan and implement encryption for email messages

- define requirements for implementing Office 365 Message Encryption
- implement Office 365 Advanced Message Encryption

Implement Data Loss Prevention (30-35%)

Create and configure data loss prevention policies

- recommend a data loss prevention solution for an organization
- configure data loss prevention for policy precedence
- configure policies for Microsoft Exchange email
- configure policies for Microsoft SharePoint sites
- configure policies for Microsoft OneDrive accounts
- configure policies for Microsoft Teams chat and channel messages
- integrate Microsoft Cloud App Security (MCAS) with Microsoft Information Protection
- configure policies in Microsoft Cloud App Security (MCAS)
- implement data loss prevention policies in test mode

Implement and monitor Microsoft Endpoint data loss prevention

- configure policies for endpoints
- configure Endpoint data loss prevention settings
- recommend configurations that enable devices for Endpoint data loss prevention policies

- monitor endpoint activities

Manage and monitor data loss prevention policies and activities

- manage and respond to data loss prevention policy violations
- review and analyze data loss prevention reports
- manage permissions for data loss prevention reports
- manage data loss prevention violations in Microsoft Cloud App Security (MCAS)

Implement Information Governance (25-30%)

Configure retention policies and labels

- create and apply retention labels
- create and apply retention label policies
- configure and publish auto-apply label policies

Manage data retention in Microsoft 365

- create and apply retention policies in Microsoft SharePoint and OneDrive
- create and apply retention policies in Microsoft Teams
- recover content in Microsoft Teams, SharePoint, and OneDrive
- recover content in Microsoft Exchange
- implement retention policies and tags in Microsoft Exchange
- apply mailbox holds in Microsoft Exchange
- implement Microsoft Exchange Online archiving policies

Implement records management in Microsoft 365

- configure labels for records management
- manage and migrate retention requirements with a file plan
- configure automatic retention using File Plan descriptors
- classify records using retention labels and policies
- implement in-place records management in Microsoft SharePoint
- configure event-based retention
- manage disposition of records