Study guide for Exam SC-400: Microsoft Information Protection Administrator

Purpose of this document

This study guide should help you understand what to expect on the exam and includes a summary of the topics the exam might cover and links to additional resources. The information and materials in this document should help you focus your studies as you prepare for the exam.

Useful links	Description
Review the skills measured as of February 1, 2023	This list represents the skills measured AFTER the date provided. Study this list if you plan to take the exam AFTER that date.
Review the skills measured prior to February 1, 2023	Study this list of skills if you take your exam PRIOR to the date provided.
Change log	You can go directly to the change log if you want to see the changes that will be made on the date provided.
How to earn the certification	Some certifications only require passing one exam, while others require passing multiple exams.
Certification renewal	Microsoft associate, expert, and specialty certifications expire annually. You can renew by passing a **free** online assessment on Microsoft Learn.
Your Microsoft Learn profile	Connecting your certification profile to Learn allows you to schedule and renew exams and share and print certificates.
Passing score	A score of 700 or greater is required to pass.
Exam sandbox	You can explore the exam environment by visiting our exam sandbox.
Request accommodations	If you use assistive devices, require extra time, or need modification to any part of the exam experience, you can request an accommodation.

Useful links	Description
Take a practice test	Are you ready to take the exam or do you need to study a bit more?

Updates to the exam

Our exams are updated periodically to reflect skills that are required to perform a role. We have included two versions of the Skills Measured objectives depending on when you are taking the exam.

We always update the English language version of the exam first. Some exams are localized into other languages, and those are updated approximately eight weeks after the English version is updated. Other available languages are listed in the **Schedule Exam** section of the **Exam Details** webpage. If the exam isn't available in your preferred language, you can request an additional 30 minutes to complete the exam.

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.

Note

Most questions cover features that are general availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Skills measured as of February 1, 2023

Audience profile

The Microsoft information protection administrator plans and implements controls that meet organizational information protection and governance requirements by using Microsoft 365 information protection services. This person is responsible for translating information protection requirements and controls into technical implementation.

They assist information technology (IT) personnel, business application owners, human resources and legal stakeholders in implementing technology solutions that support the policies and controls necessary to sufficiently address regulatory requirements for their organization. They also work with the security and governance leadership, such as a chief compliance officer, chief data 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 evaluates 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.

Candidates should have strong experience with Microsoft 365 services.

- Implement information protection (35–40%)
- Implement data loss prevention (30–35%)

- Implement information governance (25–30%)

Implement information protection (35–40%)

Create and manage sensitive information types

- Plan for 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 and use a keyword dictionary

Create and manage trainable classifiers

- Identify when to use trainable classifiers
- Design and create a trainable classifier
- Test a trainable classifier
- Retrain a classifier

Implement and manage sensitivity labels

- Design and implement roles and permissions for administering sensitivity labels
- Design and create sensitivity labels
- Configure and manage sensitivity label policies
- Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, Microsoft Power BI, and Microsoft SharePoint sites
- Configure and publish auto-labelling policies
- Monitor data classification and label usage by using label analytics tools such as Content explorer and Activity explorer
- Apply bulk classification to on-premises data by using the AIP unified labelling scanner
- Manage protection settings and marking for applied sensitivity labels
- Administer reporting, tracking, and access of sensitivity labels and protected content
- Create or extend existing sensitivity labels to Microsoft Purview

Design and implement encryption for email messages

- Design an email encryption solution based on methods available in Microsoft 365
- Implement Microsoft Purview Message Encryption
- Implement Microsoft Purview Advanced Message Encryption

Implement data loss prevention (30–35%)

Create and configure data loss prevention (DLP) policies

- Recommend a DLP solution for an organization
- Configure permissions for DLP

- Create, test, and tune DLP policies
- Configure DLP for policy and rule precedence
- Configure DLP policies for Microsoft Exchange Online, Microsoft SharePoint Online, Microsoft OneDrive, Microsoft Teams, Microsoft Power BI, and on-premises repositories
- Configure DLP policies for use in Microsoft Defender for Cloud Apps
- Configure file policies in Microsoft Defender for Cloud Apps to use DLP policies

Implement and monitor Microsoft Endpoint DLP

- Create and maintain DLP policies for endpoints
- Configure endpoint DLP settings
- Specify a deployment method for device onboarding
- Identify endpoint requirements for device onboarding
- Monitor endpoint activities
- Implement Microsoft Purview Extension

Analyze and respond to data loss prevention policies and activities

- Analyze data loss prevention reports
- Analyze data loss prevention activities by using Activity explorer
- Remediate data loss prevention policy violations in the Microsoft Purview compliance portal
- Remediate data loss prevention violations in Microsoft Defender for Cloud Apps

Implement information governance (25–30%)

Retain and delete data by using retention labels

- Plan for information retention and disposition by using retention labels
- Create retention labels
- Configure and manage adaptive scopes
- Configure and publish retention label policies
- Configure and publish auto-apply label policies

Manage data retention in Microsoft 365

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

Implement records management in Microsoft 365

- Plan for records management
- Configure labels for records management

- Manage 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 Online
- Manage event-based retention
- Manage disposition of records

Study resources

We recommend that you train and get hands-on experience before you take the exam. We offer self-study options and classroom training as well as links to documentation, community sites, and videos.

Study resources	Links to learning and documentation
Get trained	Choose from self-paced learning paths and modules or take an instructor-led course
Find documentation	Microsoft 365 security documentation Microsoft 365 Zero Trust deployment plan Microsoft Purview compliance documentation Microsoft 365 Defender documentation Learn about data loss prevention (DLP) Microsoft 365 for enterprise documentation and resources
Ask a question	Microsoft Q&A | Microsoft Docs
Get community support	Security, compliance, and identity community hub
Follow Microsoft Learn	Microsoft Learn - Microsoft Tech Community
Find a video	Exam Readiness Zone Browse other Microsoft Learn shows

Change log

Key to understanding the table: The topic groups (also known as functional groups) are in bold typeface followed by the objectives within each group. The table is a comparison between the two versions of the exam skills measured and the third column describes the extent of the changes.

Skill area prior to February 1, 2023	Skill area as of February 1, 2023	Change
Audience profile	Audience profile	No change
Implement Information Protection	**Implement information protection**	No change
Create and manage sensitive information types	Create and manage sensitive information types	No change
Create and manage trainable classifiers	Create and manage trainable classifiers	No change
Implement and manage sensitivity labels	Implement and manage sensitivity labels	No change
Design and implement encryption for email messages	Design and implement encryption for email messages	No change
Implement Data Loss Prevention	**Implement data loss prevention**	No change
Create and configure data loss prevention (DLP) policies	Create and configure data loss prevention (DLP) policies	No change
Implement and monitor Microsoft Endpoint DLP	Implement and monitor Microsoft Endpoint DLP	Minor
Analyze and respond to data loss prevention policies and activities	Analyze and respond to data loss prevention policies and activities	No change
Implement Information Governance	**Implement information governance**	No change
Retain and delete data by using retention labels	Retain and delete data by using retention labels	No change
Manage data retention in Microsoft 365	Manage data retention in Microsoft 365	No change
Implement records management in Microsoft 365	Implement records management in Microsoft 365	No change

Skills measured prior to February 1, 2023

- Implement information protection (35–40%)
- Implement data loss prevention (30–35%)
- Implement information governance (25–30%)

Implement information protection (35–40%)

Create and manage sensitive information types

- Plan for 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 and use a keyword dictionary

Create and manage trainable classifiers

- Identify when to use trainable classifiers
- Design and create a trainable classifier
- Test a trainable classifier
- Retrain a classifier

Implement and manage sensitivity labels

- Design and implement roles and permissions for administering sensitivity labels
- Design and create sensitivity labels
- Configure and manage sensitivity label policies
- Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, Microsoft Power BI, and Microsoft SharePoint sites
- Configure and publish auto-labelling policies
- Monitor data classification and label usage by using label analytics tools such as Content explorer and Activity explorer
- Apply bulk classification to on-premises data by using the AIP unified labelling scanner
- Manage protection settings and marking for applied sensitivity labels
- Administer reporting, tracking, and access of sensitivity labels and protected content
- Create or extend existing sensitivity labels to Microsoft Purview

Design and implement encryption for email messages

- Design an email encryption solution based on methods available in Microsoft 365
- Implement Microsoft Purview Message Encryption
- Implement Microsoft Purview Advanced Message Encryption

Implement data loss prevention (30–35%)

Create and configure data loss prevention (DLP) policies

- Recommend a DLP solution for an organization
- Configure permissions for DLP
- Create, test, and tune DLP policies
- Configure DLP for policy and rule precedence
- Configure DLP policies for Microsoft Exchange Online, Microsoft SharePoint Online, Microsoft OneDrive, Microsoft Teams, Microsoft Power BI, and on-premises repositories
- Configure DLP policies for use in Microsoft Defender for Cloud Apps
- Configure file policies in Microsoft Defender for Cloud Apps to use DLP policies

Implement and monitor Microsoft Endpoint DLP

- Create and maintain DLP policies for endpoints
- Configure endpoint DLP settings
- Specify a deployment method for device onboarding
- Identify endpoint requirements for device onboarding
- Monitor endpoint activities
- Implement Microsoft Compliance Extension

Analyze and respond to data loss prevention policies and activities

- Analyze data loss prevention reports
- Analyze data loss prevention activities by using Activity explorer
- Remediate data loss prevention policy violations in the Microsoft Purview compliance portal
- Remediate data loss prevention violations in Microsoft Defender for Cloud Apps

Implement information governance (25–30%)

Retain and delete data by using retention labels

- Plan for information retention and disposition by using retention labels
- Create retention labels
- Configure and manage adaptive scopes
- Configure and publish retention label policies
- Configure and publish auto-apply label policies

Manage data retention in Microsoft 365

- Create and apply retention policies for Microsoft SharePoint Online and OneDrive
- Create and apply retention policies for Microsoft Teams
- Configure preservation locks
- Recover retained content in Microsoft 365
- Implement retention policies and tags in Microsoft Exchange Online

- Apply mailbox holds in Microsoft Exchange Online
- Implement Microsoft Exchange Online archiving policies

Implement records management in Microsoft 365

- Plan for records management
- Configure labels for records management
- Manage 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 Online
- Manage event-based retention
- Manage disposition of records