SC-400T00: Administering Information Protection and Compliance in Microsoft 365

Course Details

Course Code:	SC-400T00
Duration:	4 days

Notes:

- This course syllabus should be used to determine whether the course is appropriate for the students, based on their current skills and technical training needs.
- Course content, prices, and availability are subject to change without notice.
- Terms and Conditions apply

Elements of this syllabus are subject to change.

About this course

Learn how to protect information in your Microsoft 365 deployment. This course focuses on data lifecycle management and information protection and compliance within your organization. The course covers implementation of data loss prevention policies, sensitive information types, sensitivity labels, data retention policies, Microsoft Purview Message Encryption, audit, eDiscovery, and insider risk among other related topics. The course helps learners prepare for the Microsoft Information Protection Administrator exam (SC-400).

Audience Profile

The information protection administrator translates an organization's risk and compliance requirements into technical implementation. They are responsible for implementing and managing solutions for content classification, data loss prevention (DLP), information protection, data lifecycle management, records management, privacy, risk, and compliance. They also work with other roles that are responsible for governance, data, and security to evaluate and develop policies to address an organization's risk reduction and compliance goals. This role assists workload administrators, business application owners, human resources departments, and legal stakeholders to implement technology solutions that support the necessary policies and controls.

Academy IT Pty Ltd
Level 4, 45 Grenfell Street
ADELAIDE 5000

Email: sales@academyit.com.au
Web: www.academyit.com.au

Phone: 08 7324 9800
Brian: 0400 112 083

Introduction to information protection and data lifecycle management in Microsoft Purview

Learn how Microsoft 365 information protection and data lifecycle management solutions help you protect and govern your data, throughout its lifecycle – wherever it lives, or wherever it travels.

Learning objectives

Upon completion of this module, you should be able to:

- Discuss information protection and data lifecycle management and why it's important.
- Describe Microsoft's approach to information protection and data lifecycle management.
- Define key terms associated with Microsoft's information protection and data lifecycle management solutions.

Identify the solutions that comprise information and data lifecycle management in Microsoft Purview.

Classify data for protection and governance

Learn about the information available to help you understand your data landscape and know your data.

Learning objectives

Upon completion of this module, you should be able to:

- List the components of the Data Classification solution.
- Identify the cards available on the Data Classification overview tab.
- Explain the Content explorer and Activity explorer.
- Describe how to use sensitive information types and trainable classifiers.

Create and manage sensitive information types

Learn how to use sensitive information types to support your information protection strategy.

Learning objectives

After completing this module, you'll be able to:

- Recognize the difference between built-in and custom sensitivity labels.
- Configure sensitive information types with exact data match-based classification.
- Implement document fingerprinting.
- Create custom keyword dictionaries.

Understand Microsoft 365 encryption

Learn how Microsoft 365 encrypts data-at-rest and in-transit, securely manages encryption keys, and provides key management options to customers to meet their business needs and compliance obligations.

Learning objectives

Upon completion of this module, you should be able to:

- Explain how encryption mitigates the risk of unauthorized data disclosure.
- Describe Microsoft data-at-rest and data-in-transit encryption solutions.
- Explain how Microsoft 365 implements service encryption to protect customer data at the application layer.
- Understand the differences between Microsoft managed keys and customer managed keys for use with service encryption.

Deploy Microsoft Purview Message Encryption

Learn about the different encryption methods Microsoft Purview provides to protect messages.

Learning objectives

After completing this module, you will be able to:

- Configure Microsoft Purview Message Encryption for end users
- Implement Microsoft Purview Advanced Message Encryption

Create and manage sensitivity labels with Microsoft Purview

Learn how to detect sensitive content as it's used and shared throughout your organization, in the cloud and on devices, and help prevent accidental data loss.

Learning objectives

Upon completion of this module, you should be able to:

- Discuss the information protection solution and its benefits.

- List the customer scenarios the information protection solution addresses.
- Describe the information protection configuration process.
- Explain what users will experience when the solution is implemented.
- Articulate deployment and adoption best practices.

Apply and manage sensitivity labels

Learn about how sensitivity labels are used to classify and protect business data while making sure that user productivity and their ability to collaborate aren't hindered.

Learning objectives

After completing this module, you'll be able to:

- Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites.
- Monitor label usage using label analytics.
- Configure on-premises labelling.
- Manage protection settings and marking for applied sensitivity labels.
- Apply protections and restrictions to email.
- Apply protections and restrictions to files.

Prevent data loss in Microsoft Purview

Learn how to discover, classify, and protect sensitive and business-critical content throughout its lifecycle across your organization.

Learning objectives

When you finish with this module, you'll be able to:

- Discuss the data loss prevention solution and its benefits.
- Describe the data loss prevention configuration process.
- Explain what users experience when the solution is implemented.

Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform

Learn how to configure and implement data loss prevention policies and integrate them with Microsoft Defender for Cloud Apps.

Learning objectives

After completing this module you will be able to:

- Describe the integration of DLP with Microsoft Defender for Cloud Apps.
- Configure policies in Microsoft Defender for Cloud Apps.

Manage data loss prevention policies and reports in Microsoft 365

Learn how to manage data loss prevention policies and mitigate data loss prevention policy violations.

Learning objectives

After completing this module, you'll be able to:

- Review and analyze DLP reports.
- Manage permissions for DLP reports.
- Identify and mitigate DLP policy violations.
- Mitigate DLP violations in Microsoft Defender for Cloud Apps.

Manage the data lifecycle in Microsoft Purview

Learn how to manage your content lifecycle using solutions to import, store, and classify business-critical data so you can keep what you need and delete what you don't.

Learning objectives

- Upon completion of this module, you should be able to:
- Discuss the Data Lifecycle Management solution and its benefits.
- List the customer scenarios the Data Lifecycle Management solution addresses.
- Describe the Data Lifecycle Management configuration process.
- Explain what users will experience when the solution is implemented.
- Articulate deployment and adoption best practices.

Manage data retention in Microsoft 365 workloads

Learn how to manage retention for Microsoft 365, and how retention solutions are implemented in the individual Microsoft 365 services.

Learning objectives

After completing this module, you will be able to:

- Describe the retention features in Microsoft 365 workloads.
- Configure retention settings in Microsoft Teams, Yammer, and SharePoint Online.
- Recover content protected by retention settings.
- Regain protected items from Exchange Mailboxes.

Manage records in Microsoft Purview

Learn how to use intelligent classification to automate and simplify the retention schedule for regulatory, legal, and business-critical records in your organization.

Learning objectives

Upon completion of this module, you should be able to:

- Discuss the Microsoft Purview Records Management solution and its benefits.
- List the customer scenarios the Microsoft Purview Records Management solution addresses.
- Describe the Microsoft Purview Records Management configuration process.
- Explain what users will experience when the solution is implemented.
- Articulate deployment and adoption best practices.

Explore compliance in Microsoft 365

This module explores the tools Microsoft 365 provides to help ensure an organization's regulatory compliance, including the Microsoft Purview compliance portal, Compliance Manager, and the Microsoft compliance score.

Learning objectives

By the end of this module, you should be able to:

- Describe how Microsoft 365 helps organizations manage risks, protect data, and remain compliant with regulations and standards.
- Plan your beginning compliance tasks in Microsoft Purview.
- Manage your compliance requirements with Compliance Manager.
- Manage compliance posture and improvement actions using the Compliance Manager dashboard.
- Explain how an organization's compliance score is determined.

Search for content in the Microsoft Purview compliance portal

This module examines how to search for content in the Microsoft Purview compliance portal using Content Search functionality, including how to view and export the search results, and configure search permissions filtering.

Learning objectives

By the end of this module, you'll be able to:

- Describe how to use content search in the Microsoft Purview compliance portal.
- Design and create a content search.
- Preview the search results.
- View the search statistics.
- Export the search results and search report.
- Configure search permission filtering.

Manage Microsoft Purview eDiscovery (Standard)

This module explores how to use Microsoft Purview eDiscovery (Standard) to create an eDiscovery case and a hold for a case, how to manage case content, and how to close, reopen, and delete a case.

Learning objectives

By the end of this module, you'll be able to:

- Describe how Microsoft Purview eDiscovery (Standard) builds on the basic search and export functionality of Content search.
- Describe the basic workflow of eDiscovery (Standard).
- Create an eDiscovery case.
- Create an eDiscovery hold for an eDiscovery case.
- Search for content in a case and then export that content.
- Close, reopen, and delete a case.

Manage Microsoft Purview eDiscovery (Premium)

This module explores how to use Microsoft Purview eDiscovery (Premium) to preserve, collect, analyze, review, and export content that's responsive to an organization's internal and external investigations, and communicate with custodians involved in a case.

Learning objectives

By the end of this module, you'll be able to:

- Describe how Microsoft Purview eDiscovery (Premium) builds on eDiscovery (Standard).
- Describe the basic workflow of eDiscovery (Premium).
- Create and manage cases in eDiscovery (Premium).
- Manage custodians and non-custodial data sources.
- Analyze case content and use analytical tools to reduce the size of search result sets.

Manage Microsoft Purview Audit (Standard)

This module examines how to search for audited activities using the Microsoft Purview Audit (Standard) solution, including how to export, configure, and view the audit log records that were retrieved from an audit log search.

Learning objectives

By the end of this module, you'll be able to:

- Describe the differences between Audit (Standard) and Audit (Premium).
- Identify the core features of the Audit (Standard) solution.
- Set up and implement audit log searching using the Audit (Standard) solution.
- Export, configure, and view audit log records.
- Use audit log searching to troubleshoot common support issues.

Prepare Microsoft Purview Communication Compliance

Microsoft Purview Communication Compliance is a solution that helps organizations address code-of-conduct policy violations in company communications, while also assisting organizations in regulated industries meet specific supervisory compliance requirements.

Communication Compliance uses machine learning to intelligently detect violations across different communication channels such as Microsoft Teams, Exchange Online, or Yammer messages.

Learning objectives

Upon completion of this module, you should be able to:

- List the enhancements in communication compliance over Office 365 Supervision policies, which it will replace.
- Explain how to identify and remediate code-of-conduct policy violations.
- List the prerequisites that need to be met before creating communication compliance policies.
- Describe the types of built-in, pre-defined policy templates.

Manage insider risk in Microsoft Purview

Microsoft Purview Insider Risk Management helps organizations address internal risks, such as IP theft, fraud, and sabotage. Learn about insider risk management and how Microsoft technologies can help you detect, investigate, and take action on risky activities in your organization.

Learning objectives

Upon completion of this module, you should be able to:

- Explain how Microsoft Purview Insider Risk Management can help prevent, detect, and contain internal risks in an organization.
- Describe the types of built-in, pre-defined policy templates.
- List the prerequisites that need to be met before creating insider risk policies.
- Explain the types of actions you can take on an insider risk management case.

Implement Microsoft Purview Information Barriers

This module examines how Microsoft Purview uses information barriers to restrict communication and collaboration in Microsoft Teams, SharePoint Online, and OneDrive for Business.

Learning objectives

By the end of this module, you should be able to:

- Describe how information barriers can restrict or allow communication and collaboration among specific groups of users.
- Describe the components of an information barrier and how to enable information barriers.
- Understand how information barriers help organizations determine which users to add or remove from a Microsoft Team, OneDrive account, and SharePoint site.
- Describe how information barriers prevent users or groups from communicating and collaborating in Microsoft Teams, OneDrive, and SharePoint.

Manage regulatory and privacy requirements with Microsoft Priva

Learn how to use Microsoft Priva to manage privacy risk policies and subject rights requests.

Learning objectives

Upon completion of this module, the learner will be able to:

- Create and manage risk management policies for data overexposure, data transfer, and data minimization
- Investigate and remediate risk alerts
- Send user notifications
- Create and manage Subject Rights Requests
- Estimate and retrieve subject data
- Review subject data
- Create subject rights reports

Implement privileged access management

Privileged access management allows granular access control over privileged admin tasks in Office 365. Privileged access management requires users to request just-in-time access to complete elevated and privileged tasks through a highly scoped and time-bound approval workflow. This configuration gives users just-enough-access to perform the task at hand without risking exposure of sensitive data or critical configuration settings.

Learning objectives

Upon completion of this module, you should be able to:

- Explain the difference between privileged access management and privileged identity management.
- Describe the privileged access management process flow.
- Describe how to configure and enable privileged access management.

Manage Customer Lockbox

Customer Lockbox supports requests to access data in Exchange Online, SharePoint Online, and OneDrive when Microsoft engineers need to access customer content to determine root cause and fix an issue. Customer Lockbox requires the engineer to request access from the customer as a final step in the approval workflow. This gives organizations the option to approve or deny these requests and provide direct-access control to the customer.

Learning objectives

Upon completion of this module, you should be able to:

- Describe the Customer Lockbox workflow.
- Explain how to approve or deny a Customer Lockbox request.
- Explain how you can audit actions performed by Microsoft engineers when access requests are approved.