MS-SC401T00: INFORMATION SECURITY ADMINISTRATOR

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
4 Days	Intermediate	Security	Instructor-led	NA

INTRODUCTION

The Information Security Administrator course equips you with the skills needed to plan and implement information security for sensitive data using Microsoft Purview and related services. The course covers essential topics such as information protection, data loss prevention (DLP), retention, and insider risk management. You learn how to protect data within Microsoft 365 collaboration environments from internal and external threats. Additionally, you learn how to manage security alerts and respond to incidents by investigating activities, responding to DLP alerts, and managing insider risk cases. You also learn how to protect data used by AI services within Microsoft environments and implement controls to safeguard content in these environments.

AUDIENCE PROFILE

As an Information Security Administrator, you plan and implement information security for sensitive data using Microsoft Purview and related services. You're responsible for mitigating risks by protecting data within Microsoft 365 collaboration environments from internal and external threats, as well as safeguarding data used by AI services. Your role involves implementing information protection, data loss prevention (DLP), retention, and insider risk management. You also manage security alerts and respond to incidents by investigating activities, responding to DLP alerts, and managing insider risk cases. In this role, you collaborate with other roles responsible for governance, data, and security to develop policies that address your organization's security and risk reduction goals. You work with workload administrators, business application owners, and governance stakeholders to implement technology solutions that support these policies and controls.

PREREQUISITES

Before attending this course, delegates must be familiar with:

- Microsoft 365 services and security-related tools.
- PowerShell for administrative automation.
- Microsoft Entra (formerly Azure Active Directory) for identity management.
- Microsoft Defender portal for security monitoring.
- Microsoft Defender for Cloud Apps for cloud security governance.

COURSE OBJECTIVES

After completing this course, delegates will be able to:

- Implement information protection: Safeguard sensitive data using Microsoft Purview and related services.
- Deploy data loss prevention and retention policies: Ensure compliance and secure data across collaboration environments.
- Manage risks, alerts, and activities: Respond to security incidents and mitigate threats effectively.
- Collaborate with governance and security teams: Develop policies to address organizational security goals.
- Coordinate with workload administrators and stakeholders: Implement technology solutions aligned with regulatory frameworks.

COURSE CONTENT

Module 1: Protect sensitive data in a digital world
Discover how Microsoft Purview helps organizations classify, protect, and monitor sensitive data across cloud, endpoint, and AI environments. This module explores strategies for securing data through classification, labeling, encryption, and proactive risk management.

Lessons

- Introduction
- The growing need for data protection
- The challenges of managing sensitive data
- Protect data in a Zero Trust world
- Understand data classification and protection
- Prevent data leaks and insider threats
- Manage security alerts and respond to threats

- Protect AI-generated and AI-processed data
- Module assessment
- Summary

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

- Describe challenges in protecting sensitive data across cloud and AI environments.
- Explain how Microsoft Purview enables data classification, labeling, and protection.
- Identify how data loss prevention (DLP) prevents unauthorized data sharing.
- Understand how Insider Risk Management helps detect potential threats.
- Explore security monitoring tools for detecting and responding to data risks.

Module 2: Classify data for protection and governance

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

Lessons

- Introduction
- Data classification overview
- Classify data using sensitive information types
- Classify data using trainable classifiers
- Create a custom trainable classifier
- Module assessment
- Summary

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

- Explain the importance of data classification for protection and governance.
- Describe how sensitive information types (SITs) classify structured data.
- Explain how trainable classifiers identify unstructured data.
- Create a custom trainable classifier to detect organization-specific content.

Module 3: Review and analyze data classification and protection

Discover how Microsoft Purview helps organizations monitor and analyze data classification and protection. This module explores how security teams can track classification trends, investigate labeled content, and assess policy effectiveness using Information Protection Reports, Data explorer, Content explorer, and Activity explorer.

Lessons

- Introduction
- Review classification and protection insights
- Analyze classified data with data and content explorer
- Monitor and review actions on labeled data
- Module assessment
- Summary

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

- Interpret Information Protection Reports to assess classification and protection trends.
- Investigate labeled content using Data explorer and Content explorer to identify classification patterns.
- Analyze user activity in Activity explorer to detect policy violations and potential security risks.
- Use Microsoft Purview tools to improve data security, maintain compliance, and refine protection strategies.

Module 4: Create and manage sensitive information types

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

Lessons

- Introduction
- Sensitive information type overview
- Compare built-in versus custom sensitive information types
- Create and manage custom sensitive information types
- Create and manage exact data match sensitive info types
- Implement document fingerprinting
- Describe named entities
- Create a keyword dictionary
- Module assessment
- Summary and resources

By the end of 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.

Module 5: Create and configure sensitivity labels with Microsoft Purview

Microsoft Purview sensitivity labels enable you to classify and protect sensitive data throughout your organization, including in the cloud and on devices. This module covers how to classify and protect sensitive information to ensure its security and compliance.

Lessons

- Introduction
- Sensitivity label overview
- Create and configure sensitivity labels and label policies
- Configure encryption with sensitivity labels
- Implement auto-labeling policies
- Use the data classification dashboard to monitor sensitivity labels
- Module assessment
- Summary

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

- Understand the basics of Microsoft Purview sensitivity labels in Microsoft 365.
- Create and publish sensitivity labels to classify and safeguard data.
- Configure encryption settings with sensitivity labels for improved data security.
- Implement auto-labeling for consistent data classification and protection.
- Use the Microsoft Purview data classification dashboard to monitor sensitivity label usage.

Module 6: Apply sensitivity labels for data protection

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.

Lessons

- Introduction
- Foundations of sensitivity label integration in Microsoft 365
- Manage sensitivity labels in Office apps
- Apply sensitivity labels with Microsoft 365 Copilot for secure collaboration
- Protect meetings with sensitivity labels
- Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites
- Module assessment
- Summary and resources

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

- Understand the foundations of sensitivity label integration in Microsoft 365.
- Manage sensitivity label use in Office apps for security compliance.

- Secure Outlook and Teams meetings with sensitivity labels.
- Apply labels to Microsoft 365 Groups, SharePoint, and OneDrive for data protection.

Module 7: 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.

Lessons

- Introduction to Microsoft 365 encryption
- Learn how Microsoft 365 data is encrypted at rest
- Understand service encryption in Microsoft Purview
- Explore customer key management using Customer Key
- Learn how data is encrypted in-transit
- Summary and knowledge check

By the end of this module, you'll 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.

Module 8: Deploy Microsoft Purview Message Encryption

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

Lessons

- Introduction
- Implement Microsoft Purview Message Encryption
- Implement Microsoft Purview Advanced Message Encryption
- Use Microsoft Purview Message Encryption templates in mail flow rules
- Module assessment
- Summary and resources

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

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

Module 9: Prevent data loss in Microsoft Purview

Microsoft Purview Data Loss Prevention (DLP) helps safeguard sensitive information by monitoring and preventing accidental data leaks across your organization's digital platforms. In this module, you'll learn how to plan, deploy, and adjust DLP policies to protect sensitive data in your organization, ensuring security without disrupting daily work.

Lessons

- Introduction
- Data loss prevention overview
- Plan and design DLP policies
- Understand DLP policy deployment and simulation mode
- Create and manage DLP policies
- Integrate Adaptive Protection with DLP
- Use DLP analytics (preview) to identify data risks
- Understand DLP alerts and activity tracking
- Module assessment
- Summary and resources

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

- Understand the purpose and benefits of Microsoft Purview DLP.
- Plan, design, simulate, and deploy DLP policies.
- Apply Adaptive Protection for dynamic, risk-based data controls.
- Use DLP analytics to improve policy effectiveness.
- Monitor, investigate, and refine policies using alerts and activity tracking.

Module 10: Implement endpoint data loss prevention (DLP) with Microsoft Purview

Endpoint DLP in Microsoft Purview helps organizations protect sensitive data on endpoint devices by monitoring, restricting, or allowing actions such as file transfers, copying, and sharing. Learn how to onboard devices, configure settings, and create custom policies to ensure data security across your organization.

Lessons

- Introduction
- Endpoint data loss prevention (DLP) overview
- Understand the endpoint DLP implementation workflow
- Onboard devices for endpoint DLP
- Configure settings for endpoint DLP
- Create and manage endpoint DLP policies
- Deploy the Microsoft Purview browser extension
- Configure just-in-time (JIT) protection
- Module assessment
- Summary and resources

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

- Understand the benefits of endpoint DLP
- Onboard devices for endpoint DLP
- Configure endpoint DLP settings
- Create and manage endpoint DLP policies

Module 11: 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.

Lessons

- Introduction
- Configure data loss prevention policies for Power Platform
- Integrate data loss prevention in Microsoft Defender for Cloud Apps
- Configure policies in Microsoft Defender for Cloud Apps
- Manage data loss prevention violations in Microsoft Defender for Cloud Apps
- Module assessment
- Summary and resources

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

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

Module 12: Understand Microsoft Purview Insider Risk Management

Understand insider risks and discover how Microsoft Purview Insider Risk Management identifies risky activities, analyzes context, and helps organizations protect data while respecting privacy.

Lessons

- Introduction
- What is an insider risk?
- Microsoft Purview Insider Risk Management overview
- Microsoft Purview Insider Risk Management features
- Case study: Protect sensitive data with Insider Risk Management
- Module assessment
- Summary

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

- Define insider risks and their effect on organizations.
- Understand the purpose of Microsoft Purview Insider Risk Management.

- Identify key features like policies, signals, analytics, dashboards, and investigative tools.
- Recognize how these tools detect and address potential risks.
- Explore scenarios that demonstrate effective risk management strategies.

Module 13: Prepare for Microsoft Purview Insider Risk Management

Discover strategies for planning and configuring Microsoft Purview Insider Risk Management to meet organizational needs and protect privacy.

Lessons

- Introduction
- Plan for Insider Risk Management
- Prepare your organization for Insider Risk Management
- Configure settings for Insider Risk Management
- Integrate Insider Risk Management with data sources and tools
- Module assessment
- Summary

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

- Collaborate with stakeholders to prepare for insider risk management.
- Understand what's needed to meet prerequisites for implementation.
- Configure settings to align with compliance and privacy needs.
- Explore how connecting tools and data sources enhances risk management.

Module 14: Create and manage Insider Risk Management policies

Create and manage Microsoft Purview Insider Risk Management policies to detect and address potential insider risks while supporting organizational security and privacy.

Lessons

- Introduction
- Understand Insider Risk Management policy templates
- Compare quick and custom insider risk policies
- Create a custom Insider Risk Management policy
- Manage policies in Insider Risk Management
- Module assessment
- Summary

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

- Explain the purpose of policy templates.
- Identify when to use quick or custom policies.
- Create quick policies for common scenarios.
- Build and configure custom policies for specific risks.
- Update and manage policies as organizational needs change.

Module 15: Implement Adaptive Protection in Insider Risk Management

Understand how Adaptive Protection applies machine learning to assess user risk and automatically enforce the right level of security controls. By dynamically assigning Data loss prevention, Data lifecycle management, and Conditional Access policies, it strengthens data security while reducing unnecessary alerts and manual intervention.

Lessons

- Introduction
- Adaptive Protection overview
- Understand and configure risk levels in Adaptive Protection
- Configure Adaptive Protection
- Manage Adaptive Protection
- Summary and knowledge check

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

- Describe Adaptive Protection and its role in dynamically mitigating risks.
- Configure risk level settings and customize risk levels based on your organization's needs.
- Set up Adaptive Protection with quick or custom setup.
- Manage Adaptive Protection to review policy metrics, track in-scope users, and assess risk levels.

Module 16: Discover AI interactions with Microsoft Purview

Microsoft Purview helps organizations discover how Microsoft 365 Copilot and other AI tools interact with data. Using Data Security Posture Management (DSPM) for AI and Audit, security teams can detect AI activity, assess potential risks, and gather insights to support data protection and compliance strategies.

Lessons

- Introduction
- Understand AI security risks
- Microsoft Purview Data Security Posture Management (DSPM) for AI overview
- Configure DSPM for AI
- Review AI security reports
- Audit Microsoft 365 Copilot activities and AI interactions with Microsoft Purview
- Module assessment
- Summary

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

- Explain how Microsoft Purview DSPM for AI and Audit help identify AI-related data risks
- Set up DSPM for AI to detect activity from Microsoft 365 Copilot and enterprise AI tools
- Use Microsoft Purview Audit to search for and review Copilot interactions
- Analyze AI activity and risks using built-in reports and insights

Module 17: Protect sensitive data from AI-related risks

Microsoft Purview helps organizations protect sensitive data in environments that use AI tools. Learn how to reduce data security risks by applying sensitivity labels, using data loss prevention controls, and deploying recommended protections through DSPM for AI.

Lessons

- Introduction
- Apply AI security recommendations with DSPM for AI
- Use sensitivity labels to protect Microsoft 365 Copilot content
- Use Endpoint DLP to prevent generative AI data exposure
- Module assessment
- Summary

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

- Use sensitivity labels to control how AI tools access and handle content
- Configure endpoint DLP to restrict risky actions in browsers
- Apply DSPM for AI recommendations to protect sensitive data across Microsoft Purview solutions

Module 18: Govern AI usage with Microsoft Purview

Learn how to apply policies and manage the lifecycle of AI-generated content using Microsoft Purview. This module shows how to retain, delete, investigate, and review content created in Microsoft 365 Copilot and other AI apps.

Lessons

- Introduction
- Apply retention policies to Microsoft 365 Copilot prompts and responses
- Investigate and delete Copilot interactions with Microsoft Purview eDiscovery
- Detect and manage Copilot and AI communications with Microsoft Purview
- Module assessment
- Summary

By the end of this module, you'll be able to:
- Apply retention policies to manage the lifecycle of Copilot and other AI-generated content using Data Lifecycle Management
- Investigate and delete Copilot interaction history using eDiscovery (Premium)
- Create policies to assess Copilot messages and other AI-related communications using Communication Compliance

Module 19: Assess and mitigate AI risks with Microsoft Purview
Microsoft Purview includes tools that help detect risky activity and apply policy-based protections in AI environments. This includes detecting generative AI usage, assigning user risk levels, and adjusting enforcement actions based on those levels.
Lessons
- Introduction
- Use data assessments to detect oversharing risks
- Detect risky AI usage with Insider Risk Management
- Case study: Use Adaptive Protection to respond to AI-related risk
- Module assessment
- Summary

By the end of this module, you'll be able to:
- Detect generative AI usage with Insider Risk Management
- Use risk scoring to identify users who pose a higher risk
- Apply dynamic protections with Adaptive Protection based on user behavior
- Use data assessments to identify oversharing risks in AI interactions

Module 20: Understand retention in Microsoft Purview
Microsoft Purview retention helps organizations manage how long data is kept and when it can be deleted. Learn how to apply retention strategically to meet compliance requirements, reduce risk, and protect important information throughout its lifecycle.
Lessons
- Introduction
- Overview of retention and the data lifecycle
- Understand retention labels and retention policies
- Decide when to apply retention
- Module assessment
- Summary

By the end of this module, you'll be able to:
- Identify common use cases for applying retention
- Explain how retention supports data protection alongside tools like data loss prevention
- Apply retention settings to specific users, sites, or content types
- Recognize what retention does and doesn't control

Module 21: Implement and manage retention and recovery in Microsoft Purview
Microsoft Purview helps reduce data exposure by providing tools to control how long content is kept and when it's permanently deleted. Through retention labels, policies, adaptive scopes, and recovery capabilities, organizations can apply consistent lifecycle rules across Microsoft 365 and reduce the risk of keeping unnecessary or outdated data. This approach supports both compliance and information security goals by minimizing what data is available to unauthorized access or misuse.
Lessons
- Introduction
- Plan for retention and disposition with retention labels
- Create and publish retention labels
- Create and manage auto-apply retention labels
- Create and configure adaptive scopes
- Create and configure retention policies
- Understand policy and label precedence in Microsoft Purview
- Recover content in Microsoft 365 workloads
- Module assessment
- Summary

By the end of this module, you'll be able to:
- Plan retention and disposition using retention labels.
- Create, publish, and automatically apply retention labels.
- Use adaptive scopes to target users, groups, or sites dynamically.
- Configure retention policies for Microsoft 365 workloads.
- Interpret the outcome when multiple retention settings apply.
- Restore deleted items and previous versions of content across SharePoint, OneDrive, and Teams.

Module 22: Search and investigate with Microsoft Purview Audit
Enhance data security and compliance with Microsoft Purview Audit by configuring detailed audits, managing logs, and analyzing access patterns.
Lessons
- Introduction
- Microsoft Purview Audit overview
- Configure and manage Microsoft Purview Audit
- Conduct searches with Audit (Standard)
- Audit Microsoft Copilot for Microsoft 365 interactions
- Investigate activities with Audit (Premium)
- Export audit log data
- Configure audit retention with Audit (Premium)
- Module assessment
- Summary

By the end of this module, you'll be able to:
- Identify the differences between Microsoft Purview Audit (Standard) and Audit (Premium).
- Configure Microsoft Purview Audit for optimal log management.
- Perform audits to assess compliance and security measures.
- Analyze irregular access patterns using advanced tools in Purview Audit (Premium) and PowerShell.
- Ensure regulatory compliance through strategic data management.

Module 23: 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.
Lessons
- Introduction
- Explore Microsoft Purview eDiscovery solutions
- Create a content search
- View the search results and statistics
- Export the search results and search report
- Configure search permissions filtering
- Search for and delete email messages
- Module assessment
- Summary

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.

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to write the Microsoft SC-401: Certified Information Security Administrator Associate exam.