Information Security Administrator

Course SC-401 4 Days Instructor-led, Hands-on

Introduction

Cybercrime damages are projected to reach $10.5 trillion annually by 2025. With internal and external threats growing, organizations can't afford gaps in governance, compliance, or data protection.

The SC-401 Information Security Administrator Course teaches you to plan and implement information security for sensitive data using Microsoft Purview and related services. You'll get hands-on experience with data loss prevention, insider risk management, retention, encryption, and AI safeguards, learning how to protect data across Microsoft 365, respond to security alerts, manage AI risks, and develop policies that support your organization's risk reduction goals.

This course is ideal for IT professionals and administrators responsible for information security, data protection, compliance, or risk management in Microsoft 365 environments.

At Course Completion

Upon successful completion of this course, students will have the following skills and knowledge:

- Implement information protection and DLP policies with Microsoft Purview
- Classify and secure data across Microsoft 365 and hybrid environments
- Configure and manage sensitivity labels, retention policies, and encryption
- Investigate and respond to insider risk and DLP incidents
- Protect AI-generated and AI-processed data with adaptive security controls

Prerequisites

Before attending this course, you should have the following:

- Familiarity with Microsoft Purview compliance solutions
- Basic understanding of data protection and security concepts
- Foundational knowledge of Microsoft security and compliance technologies
- Awareness of Microsoft 365 data governance capabilities

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

Outline

Module 1: 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

Module 2: Classify data for protection and governance

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

Module 3: Review and analyze data classification and protection

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

Module 4: Create and manage sensitive information types

- 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

Module 5: Create and configure sensitivity labels with Microsoft Purview

- Sensitivity label overview
- Create and configure sensitivity labels and label policies
- Configure encryption with sensitivity labels
- Implement auto-labeling policies
- Track and evaluate sensitivity label usage in Microsoft Purview
- Module assessment

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

Module 6: Apply sensitivity labels for data protection

- 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

Module 7: Classify and protect on-premises data with Microsoft Purview

- Protect on-premises files with Microsoft Purview
- Prepare your environment for the Microsoft Purview Information Protection scanner
- Configure and install the Microsoft Purview Information Protection scanner
- Run and manage the scanner
- Enforce data loss prevention policies on on-premises files
- Module assessment

Module 8: Understand 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

Module 9: Protect email with Microsoft Purview Message Encryption

- Understand message encryption
- Plan for Microsoft Purview Message Encryption
- Configure Microsoft Purview Message Encryption
- Customize encrypted email branding with Microsoft Purview
- Control encrypted email access with Advanced Message Encryption
- Use Microsoft Purview Message Encryption templates in mail flow rules
- Module assessment

Module 10: Prevent data loss in Microsoft Purview

- 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

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

- Use DLP analytics (preview) to identify data risks
- Understand DLP alerts and activity tracking
- Module assessment

Module 11: Implement endpoint data loss prevention (DLP) with Microsoft Purview

- 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

Module 12: Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform

- 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

Module 13: Investigate and respond to Microsoft Purview Data Loss Prevention alerts

- Understand data loss prevention (DLP) alerts
- Understand the DLP alert lifecycle
- Configure DLP policies to generate alerts
- Investigate DLP alerts in Microsoft Purview
- Investigate DLP alerts in Microsoft Defender XDR
- Respond to DLP alerts
- Module assessment

Module 14: Understand Microsoft Purview Insider Risk Management

- 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

Module 15: Prepare for Microsoft Purview Insider Risk Management

- 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

Module 16: Create and manage Insider Risk Management policies

- 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

Module 17: Investigate insider risk alerts and related activity

- Understand insider risk alerts and investigations
- Manage alert volume in insider risk management
- Investigate and triage insider risk alerts in Microsoft Purview
- Analyze alert context with the All risk factors tab
- Investigate activity details with the Activity explorer tab
- Review patterns over time with the User activity tab
- Investigate insider risk alerts in Microsoft Defender XDR
- Manage and take action on insider risk cases
- Module assessment

Module 18: Implement Adaptive Protection in Insider Risk Management

- Adaptive Protection overview
- Understand and configure risk levels in Adaptive Protection
- Configure Adaptive Protection
- Manage Adaptive Protection

Module 19: Discover AI interactions with Microsoft Purview

- 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

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

Module 20: Protect sensitive data from AI-related risks

- 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

Module 21: Govern AI usage with Microsoft Purview

- 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

Module 22: Assess and mitigate AI risks with Microsoft Purview

- 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

Module 23: Understand retention in Microsoft Purview

- Overview of retention and the data lifecycle
- Understand retention labels and retention policies
- Decide when to apply retention
- Module assessment

Module 24: Implement and manage retention and recovery in Microsoft Purview

- 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

Module 25: Search and investigate with Microsoft Purview Audit

- Microsoft Purview Audit overview
- Configure and manage Microsoft Purview Audit
- Conduct searches with Audit (Standard)

Contact ISInc for more information at 916.920.1700 or by visiting our website at http://www.isinc.com

- Audit Microsoft Copilot for Microsoft 365 interactions
- Investigate activities with Audit (Premium)
- Export audit log data
- Configure audit retention with Audit (Premium)
- Module assessment

Module 26: Search for content with Microsoft Purview eDiscovery

- Understand eDiscovery and content search capabilities
- Prerequisites for using eDiscovery in Microsoft Purview
- Create an eDiscovery search
- Conduct an eDiscovery search
- Export eDiscovery search results
- Module assessment