Information Security Administrator (SC-401T00)

Duration: 4 days
Audience: Professionnel TI

Who is this training for?

As an Information Security Administrator, you protect sensitive data by using Microsoft Purview and its associated services. You ensure the security of Microsoft 365 collaboration environments and the data used by artificial intelligence. Your role includes implementing information protection, data loss prevention (DLP), retention and insider risk management, and responding to security incidents and alerts. You collaborate with governance teams, administrators, and business leaders to develop and enforce technology policies and solutions to reduce risk and protect data.

Training objectives

- Plan and implement information security for sensitive data.
- Use Microsoft Purview and related services to protect data.
- Protect Microsoft 365 collaboration environments from internal and external threats.
- Implement information protection, data loss prevention (DLP), retention, and insider risk management solutions.
- Respond to security alerts and manage incidents, including cases of insider risks.
- Collaborate with governance teams, administrators, and business leaders to develop and enforce security policies.
- Implement controls and technological solutions to secure data, including those used by artificial intelligence services.

Summary

The Information Security Administrator training provides you with the skills to plan and implement information security for sensitive data using Microsoft Purview and related services. The training covers essential topics such as information protection, data loss prevention (DLP), retention, and insider risk management. You'll learn how to protect data in Microsoft 365 collaboration environments from internal and external threats. In addition, you will learn how to manage security alerts and

respond to incidents by investigating activities, responding to DLP alerts, and managing insider risk cases. You'll also learn how to protect data used by artificial intelligence services in Microsoft environments and how to implement controls to protect content in those environments.

Course outline

Module 1: Implement Information Protection in Microsoft Purview

- Learn about sensitive information types and how they work
- Identify custom sensitive information types
- Learn about formable classifiers
- Learn about document fingerprinting
- Learn about exact match analysis
- Explore automatic data protection
- Create and manage sensitive information types
- Create and train classifiers
- Create and manage sensitivity labels
- Configure auto-labeling policies
- Create and publish sensitivity label policies
- Manage sensitivity labels in Office applications
- Deploy sensitivity labels
- Exercise: Create and manage sensitive information types
- Exercise: Create and manage sensitivity labels
- Exercise: Create and publish automatic protection policies

Module 2: Implement data loss prevention in Microsoft Purview

- Learn about data loss prevention policies
- Understand DLP policies and protect sensitive data
- Create and manage DLP policies
- Set up DLP policies for email and OneDrive

- Set up DLP policies for Microsoft Teams and Power BI
- Set up DLP policies for devices and locations
- Manage and monitor incidents and alerts DLP
- Set up DLP notifications and reports
- Exercise: Create and manage DLP policies
- Exercise: Monitor and manage DLP alerts

Module 3: Manage data governance and records management in Microsoft Purview

- Learn about data governance in Microsoft Purview
- Understand retention labels and retention policies
- Create and configure retention labels
- Create and manage retention policies
- Configure retention Event-Based Retention
- Manage Records with Microsoft Purview Records Management
- Configure and Manage File Plans
- Exercise: Create and Configure Retention Labels
- Exercise: Create and Manage Retention Policies

Module 4: Implement Insider Risk Management in Microsoft Purview

- Learn about Insider Risk Management
- Understand Insider Risk Policies and Templates
- Create and Configure Risk Policies Internal
- Manage insider risk cases and alerts
- Investigate alerts and investigate activities
- Set up insider risk notifications and reports
- Exercise: Create and manage insider risk policies
- Exercise: Investigate and manage insider risk cases

Module 5: Protect data in Microsoft AI services

- Learn about Microsoft AI services and data security
- Understand protection controls for Microsoft Copilot
- Configure data protection for AI services
- Implement policies to secure AI-generated content
- Monitor and manage compliance for AI
- Exercise: Configure data protection for Microsoft Copilot

Approach and methodology

Practical and structured approach combining focused theory and guided workshops.

Participants progressively administer information security with Microsoft solutions through real-world exercises inspired by business scenarios, promoting immediate application of learning. They learn how to implement information protection, compliance, and governance strategies, as well as how to secure data and manage associated risks.

Led by a Microsoft certified trainer, the training focuses on interactivity and the development of directly transferable technical skills to strengthen security and compliance in a professional context.

Prerequisites

A general knowledge of information security Experience with Microsoft 365 An understanding of: compliance solutions risk management concepts

Recommendations

- Basics of information security (concepts, threats, data protection)
- Knowledge of Microsoft 365 and its services Notions of identity and access management (Entra ID)
- Understanding of compliance and governance concepts