

# SC-401: Administering Information Security in Microsoft 365 – Course Plan

---

## Course Overview

This course focuses on administering and managing information security and compliance solutions in Microsoft 365. Learners will gain skills to protect data, manage insider risks, implement data loss prevention, and respond to security incidents.

## Target Audience

- Microsoft 365 Administrators
- Security Administrators
- Compliance Administrators
- IT Professionals
- Candidates preparing for SC-401 certification

## Course Duration

Total Duration: 24–30 Hours (6–8 Days)

## Module 1: Introduction to Information Security & Compliance

- Information security concepts
- Microsoft 365 security & compliance overview
- Zero Trust principles
- Role of Information Security Administrator

## Module 2: Data Classification & Sensitivity Labels

- Data classification concepts
- Sensitivity labels
- Label policies
- Auto-labeling
- Encryption and content marking

## Module 3: Data Loss Prevention (DLP)

- DLP concepts and policies
- Microsoft Purview DLP
- DLP for Exchange, SharePoint, OneDrive, Teams
- Endpoint DLP
- DLP alerts and reporting

#### **Module 4: Insider Risk Management**

- Insider risk scenarios
- Policies and indicators
- Case management
- Alerts and investigations
- Privacy considerations

#### **Module 5: Information Protection & Governance**

- Retention labels and policies
- Records management
- Data lifecycle management
- eDiscovery (Standard & Premium)
- Audit (Standard & Premium)

#### **Module 6: Compliance Management**

- Microsoft Purview Compliance Manager
- Assessments and improvement actions
- Regulatory compliance
- Compliance reporting

#### **Module 7: Security Monitoring & Investigation**

- Alerts and investigations
- Microsoft 365 Defender overview
- Threat detection basics
- Incident response workflow

#### **Module 8: Implement & Manage Secure Collaboration**

- Secure collaboration in Teams
- External sharing controls
- Guest access management
- Conditional access overview

#### **Module 9: Exam Preparation**

- SC-401 exam structure
- Skills measured
- Scenario-based questions
- Practice tests and revision

#### **Hands-on Labs**

- Configure sensitivity labels
- Create and test DLP policies
- Setup insider risk policies
- Configure retention labels
- Use Compliance Manager

### **Certification Details**

Exam Code: SC-401

Duration: 120 minutes

Question Types: Case studies, MCQs

Target Role: Information Security Administrator

### **Outcome**

After completing this course, learners will be able to implement, manage, and monitor information protection, data governance, and compliance solutions in Microsoft 365.