M365 Security & Compliance Mastery: Fundamental to Advanced Strategies

Duration – 5 Days (40 Hours)

Dive into the comprehensive world of M365 security and compliance with this in-depth course, designed to take you from foundational concepts to advanced implementation. Begin by exploring core security principles, including the shared responsibility model, defense in depth, and the Zero Trust framework. Learn about critical identity concepts, plan and implement effective entitlement management, and manage privileged access with Microsoft Entra.As you progress, master the nuances of information protection, data loss prevention, and retention strategies using Microsoft Purview. Gain hands-on experience with practical exercises, from configuring sensitive information types to creating and managing eDiscovery cases.

Additionally, the course delves into the fundamentals of AI and Generative AI, with a focus on responsible AI practices. You'll also explore Microsoft Copilot for Security, including its core features, embedded experiences, and real-world use cases.By the end of the course, you'll be equipped with the skills and knowledge needed to secure, monitor, and manage M365 environments effectively, ensuring compliance and protecting sensitive data across your organization.

Prerequisites

- A basic understanding of Microsoft 365 services and administration.
- Familiarity with fundamental IT security concepts, including authentication, authorization, and encryption.
- Experience with Microsoft Azure and Active Directory is recommended.
- Basic knowledge of cloud computing and enterprise IT environments.
- Prior experience with security and compliance tools is beneficial.

Module 1: Describe security and compliance concepts

Lessons

- Introduction
- Describe the shared responsibility model
- Describe defense in depth
- Describe the Zero Trust model
- Describe encryption and hashing
- Describe governance, risk, and compliance (GRC) concepts

Module 2: Describe identity concepts

Lessons

- Introduction
- Define authentication and authorization
- Define identity as the primary security perimeter
- Describe the role of the identity provider
- Describe the concept of directory services and Active Directory
- Describe the concept of federation

Module 3: Plan and implement entitlement management

Lessons

- Introduction
- Define access packages
- **Exercise** - create and manage a resource catalogs with Microsoft Entra entitlement management
- Configure entitlement management
- **Exercise** - add terms of use acceptance report
- **Exercise** - manage the lifecycle of external users with Microsoft Entra identity governance
- Configure and manage connected organizations
- Review per-user entitlements

Module 4: Plan, implement, and manage access review

Lessons

- Introduction
- Plan for access reviews
- Create access reviews for groups and apps
- Create and configure access review programs
- Monitor access review findings
- Automate access review management tasks
- Configure recurring access reviews

Module 5: Monitor and maintain Microsoft Entra ID

Lessons

- Introduction
- Analyze and investigate sign-in logs to troubleshoot access issues
- Review and monitor Microsoft Entra audit logs
- **Exercise -** connect data from Microsoft Entra ID to Microsoft Sentinel
- Export logs to third-party security information and event management system
- Analyze Microsoft Entra workbooks and reporting
- Monitor security posture with Identity Secure Score

Module 6: Plan and implement privileged access

Lessons

- Introduction
- Define a privileged access strategy for administrative users
- Configure Privileged Identity Management for Azure resources
- **Exercise -** configure Privileged Identity Management for Microsoft Entra roles
- **Exercise -** assign Microsoft Entra roles in Privileged Identity Management
- **Exercise** - assign Azure resource roles in Privileged Identity Management
- Plan and configure Privileged Access Groups
- Analyze Privileged Identity Management audit history and reports
- Create and manage emergency access accounts

Module 7: Explore the many features of Microsoft Entra Permissions Management

Lessons

- Introduction
- A comprehensive experience for all cloud environments
- Get high level insights in the Permissions Management dashboard
- Dive deeper with the Analytics tab
- Develop a better understanding of your environment with reports
- Analyze historical data with the Audit tab
- Act on your findings with the Permissions Management Remediation tab
- Take a more proactive approach to managing with continuous monitoring
- Manage access to Microsoft Entra Permissions Management

Module 8: Create and manage sensitive information types

Lessons

- Introduction
- Compare built-in versus custom sensitive information types
- Create and manage custom sensitive information types
- Describe custom sensitive information types with exact data match
- Implement document fingerprinting
- Describe named entities
- Create keyword dictionary

Module 9: Create and configure sensitivity labels with Microsoft Purview

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 10: Prevent data loss in Microsoft Purview

Lessons

- Introduction
- Data loss prevention overview
- Identify content to protect
- Identify sensitive data with optical character recognition (preview)
- Define policy settings for your DLP policy
- Test and create your DLP policy
- Prepare Endpoint DLP
- Manage DLP alerts in the Microsoft Purview compliance portal
- View data loss prevention reports
- Implement the Microsoft Purview Extension

Module 11: Implement information protection and data loss prevention with Microsoft Purview

Lessons

- Introduction
- **Exercise** - Create a sensitive info type
- **Exercise** - Create and publish a sensitivity label
- **Exercise** - Create and assign an auto-labeling policy
- **Exercise** - Create a data loss prevention (DLP) policy

Module 12: Implement and manage retention with Microsoft Purview

Lessons

- Understand the differences between retention policies and retention labels
- Configure retention policies
- Create, publish, and automate retention labels
- Implement event-based retention
- Configure adaptive and static scopes
- Declare items as records and manage them through disposition reviews
- **Exercise** - Create a retention policy in the Microsoft Purview portal.
- **Exercise** - Create a retention policy using PowerShell.
- **Exercise** - Create a retention label.
- **Exercise** - Create a retention label policy.
- **Exercise** - Create an auto-apply retention label.

Module 13: Manage Microsoft Purview eDiscovery (Premium)

Lessons

- Explore Microsoft Purview eDiscovery (Premium)
- Implement Microsoft Purview eDiscovery (Premium)
- Create and manage an eDiscovery (Premium) case
- Analyze case content
- **Exercise** - Create a case in eDiscovery (Premium).
- **Exercise** - Create data sources.
- **Exercise** - Create a collection estimate.
- **Exercise** - Create a review set

Module 14: Prepare Microsoft Purview Communication Compliance

Lessons

- Set up communication compliance
- Investigate and remediate alerts
- Maintain communication compliance
- **Exercise** - Configure a custom communication compliance policy.
- **Exercise** - Test your custom policy.
- **Exercise** - Manage the communication compliance policy.

Module 15: Fundamental AI Concepts

Lessons

- Introduction to AI
- Understand machine learning
- Understand computer vision
- Understand natural language processing
- Understand document intelligence and knowledge mining
- Understand generative AI
- Challenges and risks with AI
- Understand Responsible AI

Module 16: Fundamentals of Generative AI

Lessons

- Introduction1 min
- What is generative AI?2 min
- What are language models?8 min
- Using language models3 min
- What are copilots?3 min
- Microsoft Copilot6 min
- Considerations for Copilot prompts3 min
- Extending and developing copilots3 min
- Exercise - Explore Microsoft Copilot

Module 17: Fundamentals of Responsible Generative AI

Lessons

- Introduction1 min
- Plan a responsible generative AI solution2 min
- Identify potential harms5 min
- Measure potential harms5 min
- Mitigate potential harms5 min
- Operate a responsible generative AI solution3 min
- Exercise - Explore content filters in Azure OpenAI

Module 18: Describe Microsoft Copilot for Security

Lessons

- Introduction
- Get acquainted with Microsoft Copilot for Security
- Describe Microsoft Copilot for Security terminology
- Describe how Microsoft Copilot for Security processes prompt requests
- Describe the elements of an effective prompt
- Describe how to enable Microsoft Copilot for Security

Module 19: Describe the core features of Microsoft Copilot for Security

Lessons

- Introduction
- Describe the features available in the standalone experience of Microsoft Copilot for Security
- Describe the features available in a session of the standalone experience
- Describe the Microsoft plugins available in Microsoft Copilot for Security
- Describe the non-Microsoft plugins supported by Microsoft Copilot for Security
- Describe custom promptbooks
- Describe knowledge base connections

Module 20: Describe the embedded experiences of Microsoft Copilot for Security

Lessons

- Introduction
- Describe Microsoft Copilot in Microsoft Defender XDR
- Microsoft Copilot in Microsoft Purview
- Microsoft Copilot in Microsoft Entra
- Microsoft Copilot in Microsoft Intune
- Microsoft Copilot in Microsoft Defender for Cloud (Preview)

Module 21: Explore use cases of Microsoft Copilot for Security

Lessons

- Introduction
- Explore the first run experience
- Explore the standalone experience
- Configure the Microsoft Sentinel plugin
- Enable a custom plugin
- Explore file uploads as a knowledge base
- Create a custom promptbook
- Explore the capabilities of Copilot in Microsoft Defender XDR
- Explore the capabilities of Copilot in Microsoft Purview