Prepare security and compliance to support Microsoft 365 Copilot #MS-4002

Overview

This learning path examines the key Microsoft 365 security and compliance features that administrators must prepare in order to successfully implement Microsoft 365 Copilot.

Duration: 1 day (2 x 3 hours)

Prerequisites

- Students should have basic functional experience with Microsoft 365 services.
- Students must have a proficient understanding of general IT practices.

Course Content

Module 1: Implement Microsoft 365 Copilot

This module examines the key tasks that administrators must complete when implementing Microsoft 365 Copilot, such as completing prerequisites, preparing data for searches, assigning Copilot licenses, and extending Copilot.

Lessons

- Introduction
- Get ready for Microsoft 365 Copilot
- Implement SharePoint Advanced Management tools to prepare for Microsoft 365 Copilot
- Prepare your data for searches in Microsoft 365 Copilot
- Protect your Microsoft 365 Copilot data with Microsoft 365 security tools
- Assign your Microsoft 365 Copilot licenses
- Extend Microsoft 365 Copilot
- Drive Microsoft 365 Copilot adoption throughout your organization
- Module assessment
- Summary

Module 2: Manage secure user access in Microsoft 365

This module examines the various features provided in the Microsoft 365 ecosystem for securing user access, such as Conditional Access policies, multifactor authentication, self-service password management, Smart Lockout policies, and security defaults.

Lessons

- Introduction
- Examine the identity and access tools used in Microsoft 365
- Manage user passwords
- Implement Conditional Access policies
- Enable pass-through authentication
- Implement multifactor authentication
- Explore passwordless authentication options
- Explore self-service password management
- Implement Microsoft Entra Smart Lockout
- Explore Security Defaults in Microsoft Entra ID
- Investigate authentication issues using sign-in logs
- Module assessment
- Summary

Module 3: Manage permissions, roles, and role groups in Microsoft 365

This module examines the use of roles and role groups in the Microsoft 365 permission model, including role management, best practices when configuring admin roles, delegating roles, and elevating privileges.

Lessons

- Introduction
- Examine the use of roles in the Microsoft 365 permission model
- Manage roles across the Microsoft 365 ecosystem
- Explore administrator roles in Microsoft 365
- Examine best practices when configuring administrative roles
- Assign admin roles to users in Microsoft 365
- Delegate admin roles to partners
- Implement role groups in Microsoft 365
- Manage permissions using administrative units in Microsoft Entra ID
- Manage SharePoint permissions to prevent oversharing of data
- Elevate privileges using Microsoft Entra Privileged Identity Management
- Module assessment
- Summary

Module 4: Deploy Microsoft 365 Apps for enterprise

This module examines how to implement the Microsoft 365 Apps for enterprise productivity suite in both user-driven and centralized deployments.

Lessons

- Introduction
- Explore Microsoft 365 Apps for enterprise functionality
- Complete a self-service installation of Microsoft 365 Apps for enterprise
- Deploy Microsoft 365 Apps for enterprise with Microsoft Configuration Manager
- Deploy Microsoft 365 Apps for enterprise from the cloud
- Deploy Microsoft 365 Apps for enterprise from a local source
- Manage updates to Microsoft 365 Apps for enterprise
- Explore the update channels for Microsoft 365 Apps for enterprise
- Manage your cloud apps using the Microsoft 365 Apps admin center
- Add Microsoft 365 Apps for enterprise to Microsoft Intune
- Deploy Microsoft 365 Apps for enterprise security baseline
- Module assessment
- Summary

Module 5: Implement Microsoft Purview Data Loss Prevention

This module examines how organizations can use Microsoft Purview Data Loss Prevention to help protect sensitive data and define the protective actions that organizations can take when a DLP rule is violated.

Lessons

- Introduction
- Plan to implement Microsoft Purview Data Loss Protection
- Implement Microsoft Purview's default DLP policies
- Design a custom DLP policy
- Create a custom DLP policy from a template
- Configure email notifications for DLP policies
- Configure policy tips for DLP policies
- Module assessment
- Summary

Module 6: Implement Microsoft Purview Data Loss Prevention

This module examines the process for implementing sensitivity labels, including applying proper administrative permissions, determining a deployment strategy, creating, configuring, and publishing labels, and removing and deleting labels.

Lessons

- Introduction
- Plan your deployment strategy for sensitivity labels
- Enable sensitivity labels for files in SharePoint and OneDrive
- Examine the requirements to create a sensitivity label
- Create sensitivity labels
- Publish sensitivity labels
- Remove and delete sensitivity labels
- Module assessment
- Summary

Module 7: Manage Microsoft 365 Copilot extensibility

This module examines the tasks that administrators must perform to manage Microsoft 365 Copilot extensibility, such as managing Copilot agents and creating and monitoring connectors.

Lessons

- Introduction
- Manage Copilot agents in integrated apps
- Create a connection between a data source and a Microsoft Graph connector
- Monitor your Microsoft Graph connectors
- Manage how Microsoft Graph connector content is displayed in Microsoft 365 Copilot
- Module assessment
- Summary