M365 Security & Compliance Mastery: Fundamental to Advanced Strategies with Power BI

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.

Required 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 beneficia

Table of contents

Module 4 - Create and manage sensitive information types

- 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 5- Create and configure sensitivity labels with Microsoft Purview

- 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 6 - Prevent data loss in Microsoft Purview

- 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 7 - Implement information protection and data loss prevention with Microsoft Purview

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

Module 8 - Implement and manage retention with Microsoft Purview

- 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
- **Labs** - Create a retention policy in the Microsoft Purview portal.
- **Labs** - Create a retention policy using PowerShell.
- **Labs** - Create a retention label.
- **Labs** - Create a retention label policy.
- **Labs** - Create an auto-apply retention label.

Module 9 - Manage Microsoft Purview eDiscovery (Premium)

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

Module 10 - Prepare Microsoft Purview Communication Compliance

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

Module 11 - Govern organizational data using Microsoft Purview Data Lifecycle Management

- Explore data governance solutions in Microsoft Purview
- Explore data management practices in Microsoft 365
- Explore retention in Microsoft 365
- **Labs** - Activate In-Place Archiving for a new user's mailbox.
- **Labs** - Create an email retention policy for test users.
- **Labs** - Create an email retention policy for all users.

Module 12 - Minimize internal risks with Microsoft Purview Insider Risk Management

- Insider risk management planning
- Insider risk management policies
- Insider risk management activities and alerts
- Insider risk management cases

Module 13 - Power BI and Purview implementation

- Why governance for Power BI
- Governance challenges
- Benefits of Purview Integration
- Risk and Compliance