End-to-End Data Protection and Governance with Microsoft Purview

Course Overview

This 5-day training program provides a comprehensive exploration of Microsoft Purview for information protection, compliance, and governance. Participants will gain practical skills in classifying and protecting sensitive data, implementing governance controls, managing insider risks, and ensuring compliance across Microsoft 365 and beyond. The course also covers emerging areas such as AI-related risks, data lineage visualization, and advanced auditing to help organizations strengthen their security posture while meeting regulatory requirements.

By the end of this training, learners will be able to:
- Implement Microsoft Purview Information Protection and Compliance solutions.
- Classify and protect sensitive data using sensitivity labels, encryption, and policies.
- Configure and monitor DLP, insider risk, and governance solutions.
- Govern AI interactions, mitigate risks, and manage AI-related data protection.
- Apply retention, audit, and compliance strategies aligned with business and regulatory needs.

Prerequisites

Participants should have:
- A basic understanding of Microsoft 365 security and compliance concepts.
- Familiarity with identity and access management principles.
- General knowledge of data governance and regulatory compliance.
- Hands-on experience with Microsoft 365 workloads (Teams, SharePoint, Exchange) is recommended.
- Prior completion of MS-900 (Microsoft 365 Fundamentals) or equivalent knowledge is helpful but not mandatory.

Course Outline

Day 1 – Core Foundations & Environment Setup

- Introduction to Microsoft Purview Information Protection

- Protecting Sensitive Data in a Digital World

- Data Classification for Protection and Governance

- Overview of Microsoft Purview Unified Catalog

- Governance Domains and Data Products

- Roles & Permissions (Admin, Owner, Steward, Reader)

- Business Concepts: Glossary, OKRs

Day 2 – Classification, Labels & Encryption

- Creating and Managing Sensitive Information Types

- Sensitivity Labels: Creation, Configuration, Application

- Microsoft 365 Encryption Fundamentals

- Deploying Microsoft Purview Message Encryption

- Data Map & Scanning

- System & Custom Classifications (Regex, Dictionary)

- Manual vs. Automated Classification

- Sensitivity Labels vs. Classification

- Best Practices for Classification

Day 3 – DLP, Insider Risk & Compliance

- Overview of Purview DLP Capabilities

- Endpoint DLP Implementation

- Configuring DLP Policies (Defender for Cloud Apps, Power Platform)

- Insider Risk Management Concepts & Policies

- Implementing Adaptive Protection

- Investigating Insider Risk Cases

- Microsoft Purview Compliance Portal Overview

- Compliance Manager & Score

- Data Loss Prevention (Governance view)

- Information Barriers

- Regulatory Readiness & Policy Tips

Day 4 – AI, Lineage & Monitoring

- Discovering AI Interactions with Purview
- Protecting Sensitive Data from AI-Related Risks
- Governing AI Usage & Mitigating Risks
- Controls for AI Content Protection
- Data Lineage Use Cases & Granularity
- Integration with ADF, Synapse, Power BI
- Visualizing Source-to-Target Flow
- REST API for Custom Lineage
- Execution Status for Root Cause Analysis

Day 5 – Retention, Audit & Wrap-Up

- Retention Concepts & Policies
- Managing Recovery Scenarios
- Aligning Retention with Compliance Requirements
- Using Purview Audit for Investigations
- Searching Content in Compliance Portal
- Analyzing Audit Logs & Reports
- Responding to Security Incidents from Audit
- Health Management & Governance Score
- Weekly Planning & Stakeholder Mapping
- Wrap-Up: Revision, Mock Test