Mastering Compliance and Security in Microsoft 365 Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Overview

- **Implement Microsoft Purview compliance and security controls throughout Microsoft 365.**
- **Designed for Microsoft 365 professionals responsible for protecting organisational data and managing compliance requirements.**
- **Each participant receives access to a real commercial Microsoft 365 tenant for practical lab exercises.**

Mastering Compliance and Security in Microsoft 365 is an in-depth **five-day course** combining instructor-led learning with extensive hands-on lab activities.

The course explores how Microsoft Purview capabilities can be implemented to support security, information protection, governance, and compliance requirements across Microsoft 365. It covers relevant functionality available through a range of Microsoft 365 subscriptions, including Business, E3, and E5.

The programme supports the key stages of the Microsoft Information Protection approach:

- Know your data
- Protect your data
- Prevent data loss
- Govern your data

Participants explore Microsoft Purview Portal, data classification, Content Search, eDiscovery, retention, SharePoint security and external sharing, Microsoft 365 Groups and Teams governance, Sensitivity Labels, Microsoft Defender for Cloud Apps, Insider Risk Management, Data Loss Prevention (DLP), auditing, and compliance management tools.

Hands-on Labs

Each participant is provided with access to a**commercial Microsoft 365 tenant for 30 days** for optional hands-on exercises.

The lab environment is populated with sample data, allowing participants to configure and implement the Microsoft Purview and Microsoft 365 security and compliance solutions introduced throughout the course.

Labs are optional and structured so that participants can select the exercises most relevant to their learning requirements.

Note: Because some Microsoft Purview services require additional processing time, certain exercises may take several hours or longer to produce results. As a result, not every lab may be completed during the five-day course. The 30-day tenant access period gives participants sufficient time to continue and complete outstanding exercises afterwards.

Prerequisites

Mastering Compliance and Security in Microsoft 365 Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Participants should have a general understanding of core Microsoft 365 technologies and an interest in the business and technical benefits that Microsoft Purview can provide for security, information protection, governance, and compliance.

Multi-Factor Authentication (MFA)

The course may require participants to use **Multi-Factor Authentication (MFA)**. Participants should therefore install Microsoft Authenticator, or another compatible authentication application, on their mobile device before attending.

Microsoft's current MFA requirements and associated security guidance should also be reviewed before the course.

The instructor demonstrates key features throughout the programme, while optional practical exercises can be completed using the 30-day Microsoft 365 tenant supplied to each participant.

Who Should Attend

This course is particularly suitable for:

- Microsoft 365 IT professionals,
- Microsoft 365 administrators,
- Information protection and security professionals,
- Compliance and governance specialists,
- Technical professionals responsible for implementing Microsoft Purview,
- Other stakeholders who need to understand how Microsoft 365 security and compliance capabilities can be implemented within their organisation.

Outline

Module 1 – Compliance Standards and Microsoft's Approach

- Microsoft's approach and commitment to compliance
- Microsoft Shared Responsibility Model
- Microsoft Cybersecurity Reference Architecture (MCRA)
- Introduction to Microsoft Purview
- Microsoft Purview Portal and PowerShell
- Purview licensing, roles, and permissions
- Entra ID administrative roles
- Microsoft Purview roles
- Administrative Units
- Entra ID Privileged Identity Management (PIM)
- PIM for Purview roles
- Entra ID Access Reviews
- Managing the continuously evolving Microsoft 365 compliance environment
- Practical user, PIM, and group exercises

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Module 2 – Microsoft 365 Search and Data Classification Concepts

- Microsoft Search
- Using SharePoint content for eDiscovery
- SharePoint columns, search schema, and content types
- Properties supported by Purview Content Search and eDiscovery
- Microsoft Syntex
- Syntex classifiers and extractors
- Sensitivity and Retention Labels
- Microsoft Purview Data Classification
- Sensitive Information Types (SITs)
- Named Entities
- Custom Sensitive Information Types
- Exact Data Match (EDM)
- Trainable Classifiers
- Microsoft Purview Data Explorer
- Practical SharePoint, Syntex, and Exact Data Matching exercises

Module 3 – Microsoft 365 Content Search

- Content Search concepts and security
- eDiscovery Administrator and Manager roles
- Configuring security filtering
- Content Search limits
- Searching Microsoft Teams content
- Targeted Collection Search
- Condition Card Builder and KQL Editor
- Previewing results and reviewing search statistics
- Managing Content Search through PowerShell
- Exporting search results
- Working with unindexed items
- Deduplication of eDiscovery results
- Searching for and purging email messages
- Managing multiple Content Searches
- Practical Microsoft 365 Content Search lab

Module 4 – Microsoft 365 eDiscovery

- Microsoft 365 eDiscovery tasks and cases
- eDiscovery security
- Compliance Boundaries
- Creating cases and managing case membership
- Preserving content using holds
- Microsoft Teams eDiscovery
- Exchange Online Litigation Hold
- Creating and running eDiscovery searches
- Exporting eDiscovery results
- Closing and deleting cases
- Practical eDiscovery lab

Module 5 – Premium eDiscovery

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- Standard versus Premium eDiscovery
- Premium eDiscovery requirements and licensing
- Roles and permissions
- Premium eDiscovery workflow
- Attorney-client privilege
- Guest Users
- Tag Templates
- Data Custodians and Non-Custodian Data Sources
- Collections and Review Sets
- Microsoft Teams data
- Importing data from outside Microsoft 365
- Data processing and error remediation
- Review Set filters, queries, and grouping
- Tagging content
- Search and analytics
- Exporting case data

Module 6 – Microsoft 365 Data Retention and Disposal

- Microsoft 365 retention options and licensing
- Retention Policies
- Adaptive and Static Retention Policies
- Adaptive Scopes
- Retention Policy Locations
- Microsoft Teams retention considerations
- Preservation Lock
- Retention Labels
- Methods for automatically applying Retention Labels
- Record Retention Labels
- Event-Driven Retention
- Disposition Reviews
- Regulatory Records
- Label Publishing and Label Policies
- Monitoring and auditing Retention Labels
- Retention management through PowerShell
- Retention precedence
- Inactive Mailboxes
- Recovering and restoring inactive mailboxes
- Practical Retention Policies and Retention Labels labs

Module 7 – SharePoint Security

- SharePoint permissions
- Team Sites and Communication Sites
- Access Requests and sharing options
- SharePoint Site Access
- Sharing sites, libraries, lists, folders, and individual items
- Advanced Permissions
- Permission Levels
- Explicit Permissions
- Permission Inheritance
- SharePoint Groups

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- Permission management through SharePoint Admin Center
- Managing SharePoint permissions with PowerShell
- SharePoint permission best practices
- Restricted Access Control
- Block Download Policies
- Site Lifecycle Management
- SharePoint Antivirus
- OneDrive Sync Client
- Malware Detection Alerts
- Practical SharePoint Security lab

Module 8 – SharePoint External Sharing

- SharePoint External Sharing
- Authenticated External User Sharing
- Anonymous Access Links
- Tenant-level external sharing administration
- Entra ID B2B One-Time Passcodes
- Pre-creating external users
- Advanced external sharing settings
- File and Folder Links
- Site-level sharing options
- Outlook Sharing Links
- Managing External Sharing with PowerShell
- External sharing alerts, auditing, and monitoring
- Practical SharePoint External Sharing lab

Module 9 – Microsoft 365 Groups and Teams

- Microsoft 365 Groups architecture
- Creating, deleting, and recovering groups
- Guest Access
- Microsoft 365 Admin Center and Entra ID B2B controls
- Controlling guest access by domain
- Microsoft 365 Groups management with PowerShell
- Controlling group creation
- Identifying and archiving obsolete groups
- Microsoft 365 Groups Governance
- Microsoft Teams Governance
- Teams roles and permissions
- Managing access to Microsoft Teams
- External Access versus Guest Access
- Practical Microsoft 365 Groups lab

Module 10 – Sensitivity Labels

- Microsoft 365 Sensitivity Labels
- Labelling files and other items
- PDF support
- Visual Marking, Watermarks, Headers, and Footers
- Encryption
- Double Key Encryption

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- Co-Authoring
- Sensitivity Labels for meetings
- Automatic labelling
- Auto-Labelling Policies
- Label assignment with Microsoft Syntex
- Microsoft Defender for Cloud Apps File Policies
- Labels for Teams, Microsoft 365 Groups, and SharePoint Sites
- Authentication Contexts
- Label Priority, Grouping, and Sublabels
- Label Policies
- Label Reports
- Data Access Governance Reports
- Troubleshooting Sensitivity Labels
- Managing Sensitivity Labels through PowerShell
- Practical Sensitivity Labels lab

Module 11 – Microsoft Defender for Cloud Apps

- Microsoft Defender for Cloud Apps overview
- Licensing and administrative roles
- Network requirements
- Automated setup
- Connecting applications
- Cloud Discovery Dashboard
- Cloud App Catalog
- App Sanctioning
- Activity Log
- User Groups
- Scoped Deployment and Privacy
- Investigations
- Files and OAuth Apps
- App Governance
- Policies
- Session Policies
- Conditional Access App Control
- Policy Templates and Alerts
- Practical Microsoft Defender for Cloud Apps lab

Module 12 – Managing Insider Risk

- Insider Risk Management concepts and scenarios
- Insider Risk Management processes and requirements
- Analytics and Data Sharing
- Detection Groups and Global Exclusions
- Intelligent Detections
- Policy Indicators and Custom Indicators
- Priority Users and Priority Physical Assets
- Privacy
- Policies, Alerts, and Cases
- Case Actions and resolution
- Insider Risk Adaptive Protection
- Forensic Evidence

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

- Insider Risk Auditing
- Communication Compliance
- Communication Compliance Policies
- Investigation and Resolution
- Information Barriers
- Information Barriers for OneDrive, SharePoint, and Teams
- Configuring user segments

Module 13 – Microsoft 365 Data Loss Prevention (DLP)

- Microsoft 365 Data Loss Prevention fundamentals
- Components of DLP Policies
- Creating DLP Policies
- Custom DLP Policies
- Policy Locations and Settings
- DLP Conditions and Actions
- User Notifications and Overrides
- Incident Reports
- Endpoint DLP
- Restricting sensitive activities in Microsoft Edge
- Device Restrictions
- File Activity Auditing and Restrictions
- Restricted Apps Activities
- DLP Activity Explorer
- DLP Alerts
- Practical Data Loss Prevention lab

Module 14 – Auditing, Alerts, Reporting, and Compliance Tools

- Microsoft 365 Auditing
- Audit Log Permissions
- Running Audit Log Searches
- Viewing and exporting audit results
- Audit Log Retention Policies
- Microsoft 365 Alerts
- Compliance Manager and Compliance Score
- Automated Testing
- Microsoft Regulations and Assessments
- Microsoft Configuration Analyzer for Microsoft Purview (CAMP)
- Microsoft 365 Secure Score
- Compliance Score and Secure Score best practices
- Practical Auditing, Alerts, Compliance Score, and Secure Score labs