Microsoft 365 Mobility & Security

Learn via: **Classroom**

Duration: **5 Day**

https://bilginc.com/en/training/microsoft-365-mobility-and-security-125-training/

Overview

This course covers three central elements of Microsoft 365 enterprise administration – Microsoft 365 security management, Microsoft 365 compliance management, and Microsoft 365 device management.

In Microsoft 365 security management, you will examine all the common types of threat vectors and data breaches facing organizations today, and you will learn how Microsoft 365's security solutions address these security threats. You will be introduced to the Microsoft Secure Score, as well as to Azure Active Directory Identity Protection. You will then learn how to manage the Microsoft 365 security services, including Exchange Online Protection, Safe Attachments, and Safe Links. Finally, you will be introduced to the various reports that monitor your security health. You will then transition from security services to threat intelligence; specifically, using Microsoft 365 Defender, Microsoft Defender for Cloud Apps, and Microsoft Defender for Endpoint.

With your Microsoft 365 security components now firmly in place, you will examine the key components of Microsoft 365 compliance management. This begins with an overview of all key aspects of data governance, including data archiving and retention, Microsoft Purview message encryption, and data loss prevention (DLP). You will then delve deeper into archiving and retention, paying particular attention to Microsoft Purview insider risk management, information barriers, and DLP policies. You will then examine how to implement these compliance features through the use of data classification and sensitivity labels. You will conclude this section by learning how to manage search and investigation in the Microsoft Purview compliance portal. You will cover Microsoft Purview Audit (Standard and Premium) and Microsoft Purview eDiscovery (Standard and Premium).

The course concludes with an in-depth examination of Microsoft 365 device management. You will begin by planning for various aspects of device management, including preparing your Windows devices for co-management, planning for mobile application management, examining Windows client deployment scenarios, Windows Autopilot deployment models, and planning your Windows client subscription strategy. Finally, you will transition from planning to implementing device management; specifically, your Windows client deployment strategy, Windows Autopilot, Mobile Device Management (MDM), device enrollment to MDM, and endpoint security in Microsoft Intune.

This course helps to prepare the student for the Microsoft exam MS-101: Microsoft 365 Mobility and Security.

Accessing your courseware and registering attendance with Microsoft

To access your Official Curriculum (MOC) course materials you will need a Microsoft.com/Learn account. In Learn you will also be able to register your completion of the event and receive your achievement badge. You will be issued with a unique code during your event.

Prerequisites

- Students should have completed a role-based administrator course such as Messaging, Teamwork, Security and Compliance, or Collaboration.
- Students should have a proficient understanding of DNS and basic functional experience with Microsoft 365 services.
- Students must have a proficient understanding of general IT practices.

Please note: This MS101 course is aimed at delegates familiar with concepts and basic administration of Microsoft 365 technologies including PowerShell. Delegates wanting a general course about administration of Office 365 and its services should consider the QAOFF365ADM course instead for a technical introduction to Office 365. In addition, the QAOff365GOV course provides an in depth exploration of Office 365 Security Governance and Compliance.

What You Will Learn

At the end of the course, the student should be able to:

- Understand Microsoft 365 Security Metrics
- Manage security services using Microsoft Defender for Office 365
- Implement threat protection using Microsoft 365 Defender
- Manage archiving, retention policies and encryption
- Implement and manage compliance in Microsoft 365
- Manage content searches and investigations
- Understand device management
- Understand Windows 10 deployment strategies
- Implement Mobile Device Management

Outline

Learning Path 1: Explore security metrics in Microsoft 365 Defender

This learning path examines the threat vectors and data breaches organizations face today in their cybersecurity landscape, and the wide range of security solutions that Microsoft 365 provides to combat those threats.

Modules in this Learning Path

- Examine threat vectors and data breaches
- Explore the Zero Trust security model
- Explore security solutions in Microsoft 365 Defender
- Examine Microsoft Secure Score
- Examine Privileged Identity Management
- Examine Azure Identity Protection

Lab: Tenant setup and Privileged Identity Management

- Initialise your Microsoft 365 tenant
- PIM administrator approval
- PIM self-approval
- PIM teammate approval

Learning Path 2: Manage your security services in Microsoft Defender for Office 365

This learning path examines how to manage the Microsoft 365 security services, with a special focus on security reporting and managing the Safe Attachments and Safe Links features in Microsoft Defender for Office 365.

Modules in this Learning Path

- Examine Exchange Online Protection
- Examine Microsoft Defender for Office 365
- Manage Safe Attachments
- Manage Safe Links

Lab: Manage Microsoft 365 security services

- Implement a Safe Attachment policy
- Implement a Safe Links policy

Learning Path 3: Implement threat protection by using Microsoft 365 Defender

This learning path examines how to manage the Microsoft 365 threat intelligence features that provide organizations with insight and protection against the internal and external cyber-attacks that threaten their tenants.

Modules in this Learning Path

- Explore threat intelligence in Microsoft 365 Defender
- Implement app protection by using Microsoft Defender for Cloud Apps
- Implement endpoint protection by using Microsoft Defender for Endpoint
- Implement threat protection by using Microsoft Defender for Office 365

Lab: Implement threat intelligence

- Prepare for alert policies
- Implement a mailbox permission alert
- Implement a SharePoint permission alert
- Test the default eDiscovery alert
- Conduct a spear phishing attack using attack simulation training
- Conduct password attacks using attack simulation training

Learning Path 4: Explore data governance and compliance in Microsoft 365

This learning path introduces you to the data governance features of Microsoft 365, which serve regulatory compliance, can facilitate eDiscovery, and are part of a business strategy to protect the integrity of the data estate.

Modules in this Learning Path

- Examine governance and compliance solutions in Microsoft Purview
- Explore archiving and records management in Microsoft 365
- Explore retention in Microsoft 365
- Explore Microsoft Purview Message Encryption

Lab: Implement data governance

- Initialize compliance
- Configure in-place archiving and retention policies
- Create message encryption rules

Learning Path 5: Implement compliance in Microsoft 365

This learning path provides instruction on implementing the Microsoft 365 data governance features, including how to calculate your compliance readiness, implement compliance solutions, and create information barriers, DLP policies, and policy tips.

Modules in this Learning Path

- Explore compliance in Microsoft 365
- Implement Microsoft Purview insider risk management
- Create information barriers in Microsoft 365
- Explore data loss prevention in Microsoft 365
- Implement data loss prevention policies

Lab: Implement DLP policies

- Manage DLP policies
- Test the DLP policy

Learning Path 6: Manage compliance in Microsoft 365

This learning path covers data classification of sensitive information, creating trainable classifiers, document fingerprinting, and creating and managing sensitivity labels.

Modules in this Learning Path

- Implement data classification of sensitive information
- Explore sensitivity labels
- Implement sensitivity labels

Lab: Implement sensitivity labels

- Implement sensitivity labels

Learning Path 7: Manage content search and investigations in Microsoft 365

This learning path provides instruction on managing content search and investigations in Microsoft 365, including how to search for content in the Microsoft Purview compliance portal, Microsoft Purview Audit, and Microsoft Purview eDiscovery.

Modules in this Learning Path

- Search for content in the Microsoft Purview compliance portal
- Manage Microsoft Purview Audit (Standard)
- Manage Microsoft Purview Audit (Premium)
- Manage Microsoft Purview eDiscovery (Standard)
- Manage Microsoft Purview eDiscovery (Premium)

Lab: Manage search and investigations

- Conduct a data search
- Investigate your Microsoft 365 data

Learning Path 8: Prepare for device management in Microsoft 365

This learning path examines how to prepare for device management in Microsoft 365, including planning your co-management strategy for Windows devices, transitioning from Configuration Manager to Intune, and planning for Mobile Application Management.

Modules in this Learning Path

- Explore device management using Microsoft Endpoint Manager
- Prepare your Windows devices for Co-management
- Plan for mobile application management

Learning Path 9: Plan your deployment strategy for Windows devices

This learning path examines the Microsoft 365 features an organization must plan for to implement its Windows devices deployment strategy, including Windows Autopilot, its Windows device subscription activation strategy, and Desktop Analytics.

Modules in this Learning Path

- Examine Windows client deployment scenarios
- Explore Windows Autopilot deployment models
- Plan your Windows client subscription activation strategy

Learning Path 10: Implement Mobile Device Management in Microsoft 365

This learning path examines how to implement Mobile Device Management (MDM) in Microsoft 365, including how to deploy MDM, how to enroll devices to MDM, and how to manage device compliance.

Modules in this Learning Path

- Explore Mobile Device Management
- Deploy Mobile Device Management
- Enroll devices to Mobile Device Management
- Manage device compliance
- Implement endpoint security in Microsoft Intune

Lab: Manage devices with Microsoft Intune

- Prepare for Mobile Device Management in Microsoft 365
- Configure Azure AD for Intune
- Create Intune Policies
- Enroll a Windows device
- Manage and Monitor a Device in Intune