Copilot for Microsoft 365 for Administrators
MS:4006

Course Name	**Copilot for Microsoft 365 for Administrators**
Course Code	**MS:4006**
Course Duration	1 Day
Course Structure	Instructor-Led
Course Overview	This course begins by examining the Microsoft Copilot for Microsoft 365 design. Its main focus, however, is on the security and compliance features that administrators must configure in their Microsoft 365 tenant to protect their company's organizational data before they implement Copilot for Microsoft 365.
Audience Profile	This course is designed for administrators, Microsoft 365 administrators, or persons aspiring to the Microsoft 365 Administrator role who have completed at least one of the Microsoft 365 role-based administrator certification paths.
Course Prerequisites	None
Course Outcome	After completing this course, students will be able to: • Describe the prerequisites for Copilot for Microsoft 365 • Explain how Copilot for Microsoft 365 works. • Prepare your data for Copilot for Microsoft 365 searches. • Assign your Copilot for Microsoft 365 licenses. • Describe how Copilot for Microsoft 365 uses proprietary business data. • Understand how Copilot for Microsoft 365 protects sensitive business data. • Enable security defaults. • Understand how roles are used in the Microsoft 365 ecosystem. • Identify how data classification of sensitive items is handled in Microsoft 365. • Create a deployment strategy for implementing sensitivity labels that satisfies your organization's requirements.

Assessment/Evaluation	This course will prepare delegates to take the MS:4006: Copilot for Microsoft 365 for Administrators Exam. Successfully passing this exam will result in the attainment of the Copilot for Microsoft 365 for Administrators Certification and Certificate of Attendance issued by IT-IQ Botswana

Course Details	
Topic	**TOPIC 1: Examine the Copilot for Microsoft 365 design.** This module examines the Microsoft Copilot for Microsoft 365 design, how it works, its service and tenant logical architecture, and how you can extend it using plugins and Microsoft Graph connectors. **Learning objectives** By the end of this module, you should be able to: • Describe the prerequisites for Copilot for Microsoft 365. • Explain how Copilot for Microsoft 365 works. • Understand the Copilot for Microsoft 365 service and tenant logical architecture. • Describe how to extend Copilot for Microsoft 365 using plugins and Microsoft Graph connectors. **TOPIC 2: Implement Copilot for Microsoft 365** This module examines the key tasks that administrators must complete when implementing Microsoft Copilot for Microsoft 365, such as completing prerequisites, preparing data for searches, and assigning Copilot for Microsoft 365 licenses. **Learning objectives** By the end of this module, you should be able to: • Identify the prerequisites for Copilot for Microsoft 365. • Prepare your data for Copilot for Microsoft 365 searches. • Assign your Copilot for Microsoft 365 licenses. • Identify Microsoft 365 security features that control oversharing of data in Copilot for Microsoft 365.

	• Drive adoption by creating a Copilot Center of Excellence. **TOPIC 3: Examine data security and compliance in Copilot for Microsoft 365** This module examines how Microsoft Copilot for Microsoft 365 adheres to existing privacy and compliance obligations, how it ensures data residency and compliance boundary, and how it protects sensitive business data. **Learning objectives** By the end of this module, you should be able to: • Describe how Copilot for Microsoft 365 uses proprietary business data. • Understand how Copilot for Microsoft 365 protects sensitive business data. • Describe how Copilot for Microsoft 365 uses Microsoft 365 isolation and access controls. • Understand how Copilot for Microsoft 365 meets regulatory compliance mandates. **TOPIC 4: 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. **Learning objectives** By the end of this module, you should be able to: • Manage user passwords. • Create Conditional Access policies. • Enable security defaults. • Describe pass-through authentication. • Enable multifactor authentication. • Describe self-service password management. • Implement Microsoft Entra Smart Lockout. **TOPIC 5: 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.

	Learning objectives By the end of this module, you should be able to: • Understand how roles are used in the Microsoft 365 ecosystem. • Describe the Azure role-based access control permission model used in Microsoft 365. • Identify the key tasks assigned to the common Microsoft 365 admin roles. • Identify best practices when configuring admin roles. • Delegate admin roles to partners. • Implement role groups in Microsoft 365. • Manage permissions using administrative units in Microsoft Entra ID. • Manage permissions in SharePoint to prevent oversharing of data. • Elevate privileges to access admin centers by using Microsoft Entra ID Privileged Identity Management. **TOPIC 6: Implement data classification of sensitive information.** This module introduces you to data classification in Microsoft 365, including how to create and train classifiers, view sensitive data using Content explorer and Activity explorer, and implement Document Fingerprinting. **Learning objectives** By the end of this module, you should be able to: • Explain the benefits and pain points of creating a data classification framework. • Identify how data classification of sensitive items is handled in Microsoft 365. • Understand how Microsoft 365 uses trainable classifiers to protect sensitive data. • Create and then retrain custom trainable classifiers. • Analyze the results of your data classification efforts in Content explorer and Activity explorer. • Implement Document Fingerprinting to protect sensitive information being sent through Exchange Online.

	TOPIC 7: Explore sensitivity labels. This module examines how sensitivity labels from the Microsoft Information Protection solution let you classify and protect your organization's data, while making sure that user productivity and collaboration isn't hindered. **Learning objectives** By the end of this module, you should be able to: • Describe how sensitivity labels let you classify and protect your organization's data. • Identify the common reasons why organizations use sensitivity labels. • Explain what a sensitivity label is and what they can do for an organization. • Configure a sensitivity label's scope. • Explain why the order of sensitivity labels in your admin center is important. • Describe what label policies can do. **TOPIC 8: Implement sensitivity labels.** 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. **Learning objectives** By the end of this module, you should be able to: • Create a deployment strategy for implementing sensitivity labels that satisfies your organization's requirements. • Enable sensitivity labels in SharePoint Online and OneDrive so they can use encrypted files. • Create and configure sensitivity labels. • Publish sensitivity labels by creating a label policy. • Identify the differences between removing and deleting sensitivity labels.