COURSE OVERVIEW

Course Name:

Copilot for Microsoft 365 for Administrators

MS-4006_A

COURSE DURATION: 1 Day

Gauteng:
3rd Floor, 34 Whitely Road
Melrose Arch
Johannesburg
2196

Gauteng:
192 on Bram
192 Bram Fischer Drive
Ferndale, Randburg
Johannesburg
2160

Cape Town:
3rd Floor, Thomas Pattullo Building
19 Jan Smuts St
Cape Town
8000

Durban:
9 Mountview Close
Broadlands
Mount Edgecombe
Durban
4302

087 941 5764
sales@impactful.co.za
impactful.co.za

COURSE OVERVIEW

This course examines Microsoft Copilot for Microsoft 365 design. The main focus is on the security and compliance features that administrators must configure in their Microsoft 365 tenant to protect their company's organisational data before they implement Copilot for Microsoft 365.

This course is designed for administrators who've completed at least one of the Microsoft 365 role-based administrator certification paths.

COURSE OBJECTIVES

By the end of this course, you will be able to:

- Ingest, clean, and transform data
- Model data for performance and scalability
- Design and create reports for data analysis
- Apply and perform advanced report analytics
- Manage and share report assets
- Create paginated reports in Power BI

DELIVERY METHOD

Our courses offer flexible delivery options:

- In-person classroom training at the Impactful training facilities in Johannesburg, Durban and Cape Town
- Virtual instructor-led training
- Nationally: On-site at the client

IMPACTFUL
Powered by LRMG

COURSE CONTENT

Module 1: Examine the Copilot for Microsoft 365 design

- Copilot for Microsoft 365 logical architecture
- Key components of Copilot for Microsoft 365
- Copilot for Microsoft 365 service and tenant architecture
- Extend Copilot for Microsoft 365 with Microsoft Graph connectors

Module 2: Implement Copilot for Microsoft 365

- 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.

Module 3: Examine data security and compliance in Copilot for Microsoft 365

- How Copilot uses proprietary business data.
- How Copilot protects sensitive business data.
- How Copilot uses Microsoft 365 isolation and access controls.
- How Copilot meets regulatory compliance mandates.

Module 4: Manage secure access in Microsoft 365

- 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.

Module 5: Manage roles and role groups in Microsoft 365

- How roles are used in the Microsoft 365 ecosystem.
- The Azure role-based access control permission model used in Microsoft 365.
- 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.
- Elevate privileges to access admin centres by using Microsoft Entra ID Privileged Identity Management.

Module 6: Explore threat intelligence in Microsoft Defender XDR

- How threat intelligence in Microsoft 365 is powered by the Microsoft Intelligent Security Graph.
- Create alerts that can identify malicious or suspicious events.
- How the automated investigation and response process works in Microsoft Defender XDR.
- How threat hunting enables security operators to identify cybersecurity threats.
- How Advanced hunting in Microsoft Defender XDR proactively inspects events in your network to locate threat indicators and entities.

Module 7: Implement data classification of sensitive information

- Benefits and pain points of creating a data classification framework.
- How data classification of sensitive items is handled in Microsoft 365.
- How Microsoft 365 uses trainable classifiers to protect sensitive data.
- Create and then retrain custom trainable classifiers.
- Analyse 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.

Module 8: Explore sensitivity labels

- How sensitivity labels let you classify and protect your organisation's data
- Common reasons why organisations use sensitivity labels
- What a sensitivity label is and what they can do for an organisation
- Configure a sensitivity label's scope
- Why the order of sensitivity labels in your admin centre is important
- What label policies can do

Module 9: Implement sensitivity labels

- Create, configure, and publish sensitivity labels
- Administrative permissions that must be assigned to compliance team members to implement sensitivity labels
- Develop a data classification framework that provides the foundation for your sensitivity labels
- Create and configure sensitivity labels
- Publish sensitivity labels by creating a label policy
- The differences between removing and deleting sensitivity labels