

AB-900T00: INTRODUCTION TO MICROSOFT 365 & AI ADMINISTRATION



DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
1 Day	Beginner	Dynamics 365	Instructor-led / VILT	N/A

INTRODUCTION

This course provides a comprehensive introduction to Microsoft 365, Copilot, and AI-powered agents. It introduces learners to the foundational concepts, core services, and administrative controls of Microsoft 365. It then builds upon this foundation by exploring how Copilot and agents can utilize AI to automate tasks, enhance collaboration, and personalize user experiences across the Microsoft 365 suite.

AUDIENCE PROFILE

This course is designed for beginning-level technical IT/Pros and novice administrators seeking foundational understanding of Microsoft 365 services and Microsoft 365 Copilot. Learners are introduced to the essential components, concepts, and capabilities they need to utilize and manage Microsoft 365, Copilot, and agents without requiring prior hands-on experience.

PREREQUISITES

- Students should have basic functional experience with Microsoft 365 services.
- Students must have a proficient understanding of general IT practices.

COURSE OBJECTIVES

After completing this course, students will be able to:

- Explore Microsoft 365 administration
- Explore Microsoft 365 Copilot and agent administration

COURSE CONTENT

Module 1: Explore Microsoft 365 security foundations

This module provides a comprehensive overview of Microsoft 365 security foundations, guiding learners through Zero Trust principles, integrated security tools, layered protection strategies, threat intelligence, identity and access management, and best practices for maintaining a secure cloud environment.

Lessons:

- Analyze the Zero Trust security model
- Implement Zero Trust in Microsoft 365
- Examine threat protection and intelligence in Microsoft 365
- Explore identity and authentication in Microsoft 365
- Manage access and permissions in Microsoft 365
- Explore identity and access management in Microsoft Entra

- Troubleshoot and monitor identity security

After completing this module, students will be able to:

- Explain the core principles of the Zero Trust security model and how they apply to Microsoft 365.
- Identify the integrated security tools and features available in Microsoft 365 for protecting identities, endpoints, data, applications, infrastructure, and networks.
- Summarize the key tasks involved in building a layered security strategy, including assessment, identity protection, endpoint compliance, data classification, threat monitoring, and user education.
- Describe Microsoft 365's threat protection and intelligence capabilities, including how they help detect,

investigate, and respond to security threats.

- Understand the fundamentals of identity and access management, including authentication, single sign-on, and role-based access control in Microsoft 365.
- Recognize best practices for troubleshooting, monitoring, and maintaining a secure Microsoft 365 environment.

Module 2: Introduction to Microsoft 365 core services and admin controls

This module introduces the Microsoft 365 admin center and basic configurations for core services like Teams, Exchange, and SharePoint.

Lessons:

- Explore the Microsoft 365 ecosystem and core service components

- Explore the Microsoft 365 admin center and key admin tools
- Examine Microsoft Exchange, Teams, and SharePoint
- Establish security, identity, and compliance foundations
- Assign admin roles using Role-Based Access Control

After completing this module, students will be able to:

- Understand how Microsoft 365 brings together tools like Exchange, Teams, SharePoint, and OneDrive under one secure and cloud connected environment.
- Use the Microsoft 365 admin center to access service management areas, perform configuration tasks, and monitor service health.
- Describe the initial setup tasks in Exchange, SharePoint, and Teams.
- Understand how identity controls, access policies, and compliance configurations protect against unauthorized access and misuse.
- Describe how to delegate permissions and responsibilities securely using predefined or custom admin roles.

Module 3: Protect and govern Microsoft 365 data

This module provides a comprehensive overview of data protection and governance in Microsoft 365, equipping learners to understand and manage sensitive information, compliance, risk, and secure collaboration

Lessons:

- Introduction to Microsoft Purview and data governance
- Identify and respond to data risks with Microsoft Purview
- Examine compliance, AI data discovery, and eDiscovery
- Explore oversharing and data access governance in SharePoint
- Explore data protection in Microsoft 365 Copilot

After completing this module, students will be able to:

- Understand the core features and benefits of Microsoft Purview for data protection, governance, and compliance in Microsoft 365.
- Identify and classify sensitive information using automated and manual tools, including sensitivity labels and trainable classifiers.
- Explain how to implement and manage data loss prevention (DLP), insider risk management, and

communication compliance policies.

- Describe best practices for data lifecycle management, including retention, archiving, and deletion of organizational data.
- Recognize and address risks related to oversharing and data access governance in SharePoint and other collaboration platforms.
- Understand how Microsoft 365 Copilot accesses and secures data, and how to monitor and control AI-driven data interactions for compliance and safety.

Module 4: Explore Microsoft 365 Copilot and agents

This module provides a comprehensive introduction to Microsoft 365 Copilot and agents, explaining their architecture, capabilities, licensing models, deployment strategies, and practical use cases.

Lessons:

- What are agents?
- Compare Microsoft 365 Copilot and agents
- Compare Microsoft 365 Copilot licensing models
- Plan and deploy Microsoft 365 Copilot and agents
- Explore real-world use cases for Copilot and agents

After completing this module, students will be able to:

- Explain the architecture and key components of Microsoft 365 Copilot, including Microsoft Graph, orchestration services, and large language models.
- Describe the differences between Copilot and agents, and identify scenarios where each is most effective for productivity and automation.
- Understand the various types of agents available in Microsoft 365, including prebuilt, custom, SharePoint, and advanced agents, and their roles in supporting business workflows.
- Summarize the licensing models and deployment strategies for Microsoft 365 Copilot and agents, including feature enablement and administrative controls.
- Recognize best practices for planning, configuring, and governing Copilot and agents to ensure security, compliance, and effective adoption.
- Identify real-world use cases for Copilot and agents and select the right tool for specific

business needs within the Microsoft 365 ecosystem.

Module 5: Perform basic administrative tasks for Microsoft 365 Copilot

This module guides administrators on how to manage Microsoft 365 Copilot, including licensing and access control, billing and usage monitoring, prompt governance, and strategies for tracking and driving user adoption.

Lessons:

- Manage Copilot licenses and pay-as-you-go billing
- Monitor and adjust pay-as-you-go Copilot usage
- Monitor Microsoft 365 Copilot usage and adoption
- Manage and govern Microsoft 365 Copilot prompts
- Apply operational best practices for Microsoft 365 Copilot

After completing this module, you will be able to:

- Manage Microsoft 365 Copilot licenses and pay-as-you-go billing.
- Monitor and adjust pay-as-you-go Copilot usage.
- Track Microsoft 365 Copilot user adoption.
- Use Copilot Analytics to monitor usage patterns and adoption trends.
- Manage and govern prompts in Microsoft 365 Copilot.
- Employ operational best practices, such as troubleshooting common issues and communicating changes to end users.

Module 6: Perform basic administrative tasks for Microsoft 365 Copilot agents

This module guides administrators through configuring user access and permissions for agents, creating, editing, testing, and publishing Copilot agents, managing agent approval and governance, and monitoring the full lifecycle of agents using Microsoft 365 and Power Platform tools.

Lessons

- Create a Microsoft 365 Copilot Chat agent - Part 1
- Create a Microsoft 365 Copilot Chat agent - Part 2
- Create a SharePoint agent
- Test and edit your agents
- Manage user access and permissions for agents
- Examine agent approval and governance
- Monitor and manage the agent lifecycle

After completing this module, you will be able to:

- | | | |
|--|--|--|
| <ul style="list-style-type: none">– Create a Microsoft 365 Copilot Chat agent.– Create a SharePoint agent.– Test, edit, and publish agents | <ul style="list-style-type: none">– Manage user access and permissions for agents.– Manage the agent approval process and governance policies for agent deployment. | <ul style="list-style-type: none">– Monitor and manage the agent lifecycle using Microsoft 365 and Power Platform tools. |
|--|--|--|

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to write the Microsoft AB-900: Copilot & Agent Administration Fundamentals Exam.