Training: Microsoft
MS-102T00 Microsoft 365 Administrator

Gold Microsoft Partner

TRAINING GOALS:

This course covers the following key elements of Microsoft 365 administration: Microsoft 365 tenant management, Microsoft 365 identity synchronization, and Microsoft 365 security and compliance.

In Microsoft 365 tenant management, you learn how to configure your Microsoft 365 tenant, including your organizational profile, tenant subscription options, component services, user accounts and licenses, security groups, and administrative roles. You then transition to configuring Microsoft 365, with a primary focus on configuring Office client connectivity. Finally, you explore how to manage user-driven client installations of Microsoft 365 Apps for enterprise deployments.

The course then transitions to an in-depth examination of Microsoft 365 identity synchronization, with a focus on Microsoft Entra Connect and Connect Cloud Sync. You learn how to plan for and implement each of these directory synchronization options, how to manage synchronized identities, and how to implement password management in Microsoft 365 using multifactor authentication and self-service password management.

In Microsoft 365 security management, you begin examining the common types of threat vectors and data breaches facing organizations today. You then learn how Microsoft 365's security solutions address each of these threats. You are introduced to the Microsoft Secure Score, as well as to Microsoft Entra ID Protection. You then learn how to manage the Microsoft 365 security services, including Exchange Online Protection, Safe Attachments, and Safe Links. Finally, you are introduced to the various reports that monitor an organization's security health. You then transition from security services to threat intelligence; specifically, using Microsoft 365 Defender, Microsoft Defender for Cloud Apps, and Microsoft Defender for Endpoint.

Once you have this understanding of Microsoft 365's security suite, you then 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 then delve deeper into archiving and retention, paying particular attention to Microsoft Purview insider risk management, information barriers, and DLP policies. You then examine how to implement these compliance features by using data classification and sensitivity labels.

WHO SHOULD ATTEND?

This course is designed for persons aspiring to the Microsoft 365 Administrator role and have completed at least one of the Microsoft 365 role-based administrator certification paths.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

CONSPECT:

- Configure your Microsoft 365 experience
  - Configure your company’s organization profile, which is essential for setting up for your company’s tenant.
  - Maintain minimum subscription requirements for your company.
  - Manage your services and add-ins by assigning more licenses, purchasing more storage, and so on.
  - Create a checklist that enables you to confirm your Microsoft 365 tenant meets your business needs.
- Manage users, licenses, and mail contacts in Microsoft 365
  - Identify which user identity model best suited for your organization.
  - Create user accounts from both the Microsoft 365 admin center and Windows PowerShell.
  - Manage user accounts and licenses in Microsoft 365.
  - Recover deleted user accounts in Microsoft 365.
  - Perform bulk user maintenance in Azure Active Directory.
  - Create and manage mail contacts from both the new Exchange admin center and Exchange Online PowerShell.
- Manage groups in Microsoft 365
  - Describe the various types of groups available in Microsoft 365.
  - Create and manage groups using the Microsoft 365 admin center and Windows PowerShell.
  - Create and manage groups in Exchange Online and SharePoint Online.
- Add a custom domain in Microsoft 365
  - Identify the factors that must be considered when adding a custom domain to Microsoft 365.
  - Plan the DNS zones used in a custom domain.
  - Plan the DNS record requirements for a custom domain.
  - Add a custom domain to your Microsoft 365 deployment.
- Configure client connectivity to Microsoft 365
  - Describe how Outlook uses Autodiscover to connect an Outlook client to Exchange Online.
  - Identify the DNS records needed for Outlook and other Office-related clients to automatically locate the services in Microsoft 365 using the Autodiscover process.
  - Describe the connectivity protocols that enable Outlook to connect to Microsoft 365.
  - Identify the tools that can help you troubleshoot connectivity issues in Microsoft 365 deployments.
- Configure administrative roles in Microsoft 365

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Describe the Azure RBAC permission model used in Microsoft 365.
- Describe the most common Microsoft 365 admin roles.
- Identify the key tasks assigned to the common Microsoft 365 admin roles.
- Delegate admin roles to partners.
- Manage permissions using administrative units in Azure Active Directory.
- Elevate privileges to access admin centers by using Azure AD Privileged Identity Management.

- Manage tenant health and services in Microsoft 365
  - Monitor your organization's Microsoft 365 service health in the Microsoft 365 admin center.
  - Develop an incident response plan to deal with incidents that may occur with your Microsoft 365 service.
  - Request assistance from Microsoft to address technical, pre-sales, billing, and subscription support issues.
- Deploy Microsoft 365 Apps for enterprise
  - Describe the Microsoft 365 Apps for enterprise functionality.
  - Configure the Readiness Toolkit.
  - Plan a deployment strategy for Microsoft 365 Apps for enterprise.
  - Complete a user-driven installation of Microsoft 365 Apps for enterprise.
  - Deploy Microsoft 365 Apps for enterprise with Microsoft Endpoint Configuration Manager.
  - Identify the mechanisms for managing centralized deployments of Microsoft 365 Apps for enterprise.
  - Deploy Microsoft 365 Apps for enterprise with the Office Deployment Toolkit.
  - Describe how to manage Microsoft 365 Apps for enterprise updates.
  - Determine which update channel and application method applies for your organization.
- Analyze your Microsoft 365 workplace data using Microsoft Viva Insights
  - Identify how Microsoft Viva Insights can help improve collaboration behaviors in your organization.
  - Discover the sources of data used in Microsoft Viva Insights.
  - Explain the high-level insights available through Microsoft Viva Insights.
  - Create custom analysis with Microsoft Viva Insights.
  - Summarize tasks and considerations for setting up Microsoft Viva Insights and managing privacy.
- Explore identity synchronization
  - Describe the Microsoft 365 authentication and provisioning options
  - Explain the two identity models in Microsoft 365 - cloud-only identity and hybrid identity
  - Explain the three authentication methods in the hybrid identity model - Password hash synchronization, Pass-through authentication, and federated authentication

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Describe how Microsoft 365 commonly uses directory synchronization
- Prepare for identity synchronization to Microsoft 365
  - Identify the tasks necessary to configure your Azure Active Directory environment.
  - Plan directory synchronization to synchronize your on-premises Active Directory objects to Azure AD.
  - Identify the features of Azure AD Connect sync and Azure AD Connect Cloud Sync.
  - Choose which directory synchronization best fits your environment and business needs.
- Implement directory synchronization tools
  - Configure Azure AD Connect and Azure AD Connect Cloud Sync prerequisites
  - Set up Azure AD Connect and Azure AD Connect Cloud Sync
  - Monitor synchronization services using Azure AD Connect Health
- Manage synchronized identities
  - Ensure users synchronize efficiently
  - Manage groups with directory synchronization
  - Use Azure AD Connect Sync Security Groups to help maintain directory synchronization
  - Configure object filters for directory synchronization
  - Troubleshoot directory synchronization using various troubleshooting tasks and tools
- Manage secure user access in Microsoft 365
  - Manage user passwords
  - Describe pass-through authentication
  - Enable multifactor authentication
  - Describe self-service password management
  - Implement Azure AD Smart Lockout
  - Implement entitlement packages in Azure AD Identity Governance
  - Implement conditional access policies
  - Create and perform an access review
- Examine threat vectors and data breaches
  - Describe techniques hackers use to compromise user accounts through email
  - Describe techniques hackers use to gain control over resources
  - Describe techniques hackers use to compromise data
  - Mitigate an account breach
  - Prevent an elevation of privilege attack
  - Prevent data exfiltration, data deletion, and data spillage
- Explore the Zero Trust security model
  - Describe the Zero Trust approach to security in Microsoft 365
  - Describe the principles and components of the Zero Trust security model

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Describe the five steps to implementing a Zero Trust security model in your organization
- Explain Microsoft's story and strategy around Zero Trust networking

- Explore security solutions in Microsoft Defender XDR
  - Identify the features of Microsoft Defender for Office 365 that enhance email security in a Microsoft 365 deployment
  - Explain how Microsoft Defender for Identity identifies, detects, and investigates advanced threats, compromised identities, and malicious insider actions directed at your organization
  - Explain how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats
  - Describe how Microsoft 365 Threat Intelligence can be beneficial to your organization’s security officers and administrators
  - Describe how Microsoft Cloud App Security enhances visibility and control over your Microsoft 365 tenant through three core areas
- Examine Microsoft Secure Score
  - Describe the benefits of Secure Score and what kind of services can be analyzed
  - Describe how to collect data using the Secure Score API
  - Describe how to use the tool to identify gaps between your current state and where you would like to be regarding security
  - Identify actions that increase your security by mitigating risks
  - Explain where to look to determine the threats each action mitigates and the impact it has on users
- Examine Privileged Identity Management
  - Describe how Privileged Identity Management enables you to manage, control, and monitor access to important resources in your organization
  - Configure Privileged Identity Management for use in your organization
  - Describe how Privileged Identity Management audit history enables you to see all the user assignments and activations within a given time period for all privileged roles
  - Explain how Microsoft Identity Manager helps organizations manage the users, credentials, policies, and access within their organizations and hybrid environments
  - Explain how Privileged Access Management provides granular access control over privileged admin tasks in Microsoft 365
- Examine Microsoft Entra ID Protection
  - Describe Azure Identity Protection (AIP) and what kind of identities can be protected
  - Enable the three default protection policies in AIP
  - Identify the vulnerabilities and risk events detected by AIP
  - Plan your investigation in protecting cloud-based identities
  - Plan how to protect your Azure Active Directory environment from security breaches
- Examine email protection in Microsoft 365

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Describe how Exchange Online Protection analyzes email to provide anti-malware pipeline protection.
- List several mechanisms used by Exchange Online Protection to filter spam and malware.
- Describe other solutions administrators might implement to provide extra protection against phishing and spoofing.
- Understand how EOP provides protection against outbound spam.

- Enhance your email protection using Microsoft Defender for Office 365
  - Describe how the Safe Attachments feature in Microsoft Defender for Office 365 blocks zero-day malware in email attachments and documents.
  - Describe how the Safe Links feature in Microsoft Defender for Office 365 protects users from malicious URLs embedded in email and documents that point to malicious websites.
  - Create outbound spam filtering policies.
  - Unblock users who violated spam filtering policies so they can resume sending emails.
- Manage Safe Attachments
  - Create and modify a Safe Attachments policy using Microsoft 365 Defender
  - Create a Safe Attachments policy by using PowerShell
  - Configure a Safe Attachments policy
  - Describe how a transport rule can disable a Safe Attachments policy
  - Describe the end-user experience when an email attachment is scanned and found to be malicious
- Manage Safe Links
  - Create and modify a Safe Links policy using Microsoft 365 Defender
  - Create a Safe Links policy using PowerShell
  - Configure a Safe Links policy
  - Describe how a transport rule can disable a Safe Links policy
  - Describe the end-user experience when Safe Links identifies a link to a malicious website embedded in email, and a link to a malicious file hosted on a website
- Explore threat intelligence in Microsoft Defender XDR
  - Describe how threat intelligence in Microsoft 365 is powered by the Microsoft Intelligent Security Graph.
  - Create alerts that can identify malicious or suspicious events.
  - Understand how the automated investigation and response process works in Microsoft Defender XDR.
  - Describe how threat hunting enables security operators to identify cybersecurity threats.
  - Describe how Advanced hunting in Microsoft Defender XDR proactively inspects events in your network to locate threat indicators and entities.
- Implement app protection by using Microsoft Defender for Cloud Apps
  - Describe how Microsoft Defender for Cloud Apps provides improved visibility into network cloud activity and increases the protection of critical data across cloud applications.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Explain how to deploy Microsoft Defender for Cloud Apps.
- Control your cloud apps with file policies.
- Manage and respond to alerts generated by those policies.
- Configure and troubleshoot Cloud Discovery.

- Implement endpoint protection by using Microsoft Defender for Endpoint
  - Describe how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats.
  - Onboard supported devices to Microsoft Defender for Endpoint.
  - Implement the Threat and Vulnerability Management module to effectively identify, assess, and remediate endpoint weaknesses.
  - Configure device discovery to help find unmanaged devices connected to your corporate network.
  - Lower your organization's threat and vulnerability exposure by remediating issues based on prioritized security recommendations.
- Implement threat protection by using Microsoft Defender for Office 365
  - Describe the protection stack provided by Microsoft Defender for Office 365.
  - Understand how Threat Explorer can be used to investigate threats and help to protect your tenant.
  - Describe the Threat Tracker widgets and views that provide you with intelligence on different cybersecurity issues that might affect your company.
  - Run realistic attack scenarios using Attack Simulator to help identify vulnerable users before a real attack impacts your organization.
- Examine data governance solutions in Microsoft Purview
  - Protect sensitive data with Microsoft Purview Information Protection.
  - Govern organizational data using Microsoft Purview Data Lifecycle Management.
  - Minimize internal risks with Microsoft Purview Insider Risk Management.
  - Explain the Microsoft Purview eDiscovery solutions.
- Explore archiving and records management in Microsoft 365
  - Enable and disable an archive mailbox in the Microsoft Purview compliance portal and through Windows PowerShell.
  - Run diagnostic tests on an archive mailbox.
  - Learn how retention labels can be used to allow or block actions when documents and emails are declared records.
  - Create your file plan for retention and deletion settings and actions.
  - Determine when items should be marked as records by importing an existing plan (if you already have one) or create new retention labels. Restore deleted data in Exchange Online and SharePoint Online.
- Explore retention in Microsoft 365
  - Explain how a retention policies and retention labels work.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Identify the capabilities of both retention policies and retention labels.
- Select the appropriate scope for a policy depending on business requirements.
- Explain the principles of retention.
- Identify the differences between retention settings and eDiscovery holds.
- Restrict retention changes by using preservation lock.

- Explore Microsoft Purview Message Encryption
  - Describe the features of Microsoft Purview Message Encryption.
  - Explain how Microsoft Purview Message Encryption works and how to set it up.
  - Define mail flow rules that apply branding and encryption templates to encrypt email messages.
  - Add organizational branding to encrypted email messages.
  - Explain the extra capabilities provided by Microsoft Purview Advanced Message Encryption.
- Explore compliance in Microsoft 365
  - Describe how Microsoft 365 helps organizations manage risks, protect data, and remain compliant with regulations and standards.
  - Plan your beginning compliance tasks in Microsoft Purview.
  - Manage your compliance requirements with Compliance Manager.
  - Manage compliance posture and improvement actions using the Compliance Manager dashboard.
  - Explain how an organization's compliance score is determined.
- Implement Microsoft Purview Insider Risk Management
  - Describe insider risk management functionality in Microsoft 365.
  - Develop a plan to implement the Microsoft Purview Insider Risk Management solution.
  - Create insider risk management policies.
  - Manage insider risk management alerts and cases.
- Implement Microsoft Purview Information Barriers
  - Describe how information barriers can restrict or allow communication and collaboration among specific groups of users.
  - Describe the components of an information barrier and how to enable information barriers.
  - Understand how information barriers help organizations determine which users to add or remove from a Microsoft Team, OneDrive account, and SharePoint site.
  - Describe how information barriers prevent users or groups from communicating and collaborating in Microsoft Teams, OneDrive, and SharePoint.
- Explore Microsoft Purview Data Loss Prevention
  - Describe how Data Loss Prevention (DLP) is managed in Microsoft 365
  - Understand how DLP in Microsoft 365 uses sensitive information types and search

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

patterns
    - Describe how Microsoft Endpoint DLP extends the DLP activity monitoring and protection capabilities.
    - Describe what a DLP policy is and what it contains
    - View DLP policy results using both queries and reports
- Implement Microsoft Purview Data Loss Prevention
    - Create a data loss prevention implementation plan. Implement Microsoft 365's default DLP policy.
    - Create a custom DLP policy from a DLP template and from scratch.
    - Create email notifications and policy tips for users when a DLP rule applies.
    - Create policy tips for users when a DLP rule applies
    - Configure email notifications for DLP policies
- Implement data classification of sensitive information
    - 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.
- Explore sensitivity labels
    - 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
- Implement sensitivity labels
    - Describe the overall process to create, configure, and publish sensitivity labels
    - Identify the 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
    - Identify the differences between removing and deleting sensitivity labels

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

REQUIREMENTS:

Before attending this course, students must have:

- Completed a role-based administrator course such as Messaging, Teamwork, Security, Compliance, or Collaboration.
- A proficient understanding of DNS and basic functional experience with Microsoft 365 services.
- A proficient understanding of general IT practices.
- A working knowledge of PowerShell.

Difficulty level

CERTIFICATE:

The participants will obtain Microsoft certificates.

TRAINER:

Microsoft Certified Trainer.

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007