skilltec training

Moving forward in knowledge and training

Microsoft 365
Training Course Brochure

☎ 01752 227330
✉ enquiries@skilltec.co.uk
⌂ www.skilltec.co.uk

skilltec training

Moving forward in knowledge and training

Microsoft 365 Training Course Brochure

skilltec training
Moving forward in knowledge and training

Microsoft 365 Identity & Services

Course Code	MS100
Duration	5 days

Overview

This course covers three central elements of Microsoft 365 enterprise administration – Microsoft 365 tenant and service management, Office 365 management, and Microsoft 365 identity management. In Microsoft 365 tenant and service management, you will examine all the key components that must be planned for when designing your Microsoft 365 tenant. Once this planning phase is complete, you will learn how to configure your Microsoft 365 tenant, including your organizational profile, tenant subscription options, component services, user accounts and licenses, and security groups. Finally, you will learn how to manage your tenant, which includes the configuration of tenant roles and managing your tenant health and services.

With your Microsoft 365 tenant now firmly in place, you will examine the key components of Office 365 management. This begins with an overview of Office 365 product functionality, including Exchange Online, SharePoint Online, Microsoft Teams, Microsoft Power Platform, additional product resources, and device management. You will then transition to configuring Office 365, with a primary focus on configuring Office client connectivity. Finally, you will examine how to manage Microsoft 365 Apps for enterprise (formerly Office 365 ProPlus) deployments, from user-driven client installations to centralized deployments. You will wrap up this section by learning how to configure Office Telemetry and Microsoft Analytics.

The course concludes with an in-depth examination of Microsoft 365 identity synchronization, with a focus on Azure Active Directory Connect. You will learn how to plan for and implement Azure AD Connect, how to manage synchronized identities, and how to implement password management in Microsoft 365 using multi-factor authentication and self-service password management. This section wraps up with a comprehensive look at implementing application and external access. You will learn how to add and manage applications in Azure Active Directory, including how to configure multi-tenant applications. You will then examine how to configure Azure AD Application Proxy, including how to install and register a connector and how to publish an on-premises app for remote access. Finally, you will examine how to design and manage solutions for external access. This includes licensing guidance for Azure AD B2B collaboration, creating a collaborative user, and troubleshooting a B2B collaboration.

Audience

This course is designed for persons who are aspiring to the Microsoft 365 Enterprise Admin role and have completed one of the Microsoft 365 role-based administrator certification paths.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Designing, configuring, and managing your Microsoft 365 tenant.
- Office 365 product functionality.
- Configuring Office 365.
- Managing Office 365 ProPlus deployments.
- Planning and implementing identity synchronization.
- Implementing application and external access

Prerequisites

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

Course Contents

Module 1: Designing Your Microsoft 365 Tenant

This module focuses on planning your Microsoft 365 experience. This includes planning for the proper Microsoft 365 subscription, planning for Microsoft 365 in your on-premises infrastructure, planning which identity and authentication solution best fits your organizational requirements, planning your service setup, planning for hybrid environments, and planning your migration to Microsoft 365.

Lessons

- Planning your Microsoft 365 Experience
- Planning Microsoft 365 in your On-premises Infrastructure
- Planning Your Identity and Authentication Solution
- Planning Your Service Setup
- Planning Your Hybrid Environment
- Planning Your Migration to Office 365

Lab: Transition to Microsoft 365

- Transition to Microsoft 365

After completing this module, delegates will be able to:

- Determine which Microsoft 365 subscription offering best suits your organization’s requirements.
- Understand how to best use Microsoft 365 component services to meet your organizational needs.
- Plan your Microsoft 365 subscription.
- Identify the steps necessary to successfully migrate existing data to Microsoft 365.
- Prepare your organization for Microsoft 365.
- Estimate your network's bandwidth.
- Test your existing network using the tools provided by Microsoft.
- Describe the best practices for integrating to Microsoft 365.
- Identify the different deployment strategies for implementing Microsoft 365 services.
- Describe authentication behaviour when connecting with or without modern authentication.
- Explain multi-factor authentication in Microsoft 365 deployments.
- Create a plan for directory synchronization and Azure AD Connect Pass-through authentication.
- Describe the issues, benefits, and best practices when implementing ADFS.
- Plan for Azure AD Seamless Single Sign-On.
- Plan your Email migration to Office 365.
- Plan your file storage and collaboration requirements.
- Plan your Microsoft Teams environment.
- Plan for user and group synchronization using Azure AD Connect.
- Plan for hybrid Exchange, SharePoint, and Skype for Business environments.
- Plan your deployment using the Deployment Planning Checklist.
- Analyze your Active Directory and plan any necessary clean-up using the ID Fix tool.
- Determine which migration strategy to use to move your mail, calendar, and contact information.
- Describe the performance and network issues to consider when planning your migration strategy.

Module 2: Configuring Your Microsoft 365 Tenant
While Module 1 focuses on planning your Microsoft 365 tenant, this module transitions to configuring your tenant. This includes configuring your Microsoft 365 experience, including your organization profile, your tenant subscription, your services and add-ins, and your tenant configuration. You will then learn how to manage Microsoft 365 user accounts and licenses, security groups, and domain services. You will conclude by examining how to leverage FastTrack and partner services.

Lessons

- Configuring your Microsoft 365 Experience
- Managing User Accounts and Licenses in Microsoft 365
- Managing Security Groups in Microsoft 365
- Implementing Your Domain Services
- Leveraging FastTrack and Partner Services

Lab: Configure your Microsoft 365 Tenant

- Initialize your Microsoft 365 Tenant
- Manage Users and Groups
- Add a Custom Domain

After completing this module, delegates will be able to:

- Complete your company's organization profile.
- Maintain minimum subscription requirements for your company.
- Manage your services and add-ins.
- Describe the user identities in Microsoft 365.
- Create user accounts from both the Microsoft 365 admin center and in Windows PowerShell.
- Manage user accounts and licenses.
- Recover deleted user accounts.
- Describe the various types of groups available in Microsoft 365.
- Create and manage groups from Microsoft 365 admin center and using Windows PowerShell.
- Implement your domain services.
- Plan DNS for custom domains.
- Identify DNS record requirements for custom domains.
- Add a custom domain to Microsoft 365.
- Describe how FastTrack for Microsoft 365 helps customers deploy Microsoft 365.
- Request a partner to assist you with the FastTrack process.

Module 3: Managing Your Microsoft 365 Tenant

In the prior modules, you learned how to plan for and configure your Microsoft 365 tenant. In this module, you will take the next step in the deployment process by learning how to manage your tenant once it has been implemented. This includes configuring your Microsoft 365 administrator roles, managing tenant health and services, and managing user-driven and centralized deployments of Microsoft 365 Apps for enterprise (formerly Office 365 ProPlus).

Lessons

- Configuring Microsoft 365 Admin Roles
- Managing Tenant Health and Services
- Managing User-Driven Client Installations
- Managing Centralized Microsoft 365 Apps for enterprise Deployments

Lab: Manage Your Microsoft 365 Tenant

- Manage Administration Delegation
- Monitor and Troubleshoot Microsoft 365
- Install Microsoft 365 Apps for enterprise

After completing this module, delegates will be able to:

- Describe the key admin roles in Microsoft 365.
- Identify the key responsibilities of the primary admin roles.
- Configure tenant roles.
- Monitor your organization's Microsoft 365 service health in the Microsoft 365 admin center.
- Develop an incident response plan to deal with incidents in your Microsoft 365 services.
- Request assistance from Microsoft to address technical, pre-sales, billing, and subscription support.
- Describe how Microsoft 365 Apps for enterprise click-to-run technology works.
- Describe the Microsoft 365 Apps for enterprise licensing and activation processes.
- Plan which update branch might be applicable for your organization.
- Plan which method to use for applying update branches to your users.
- Identify typical obstacles that prevent successful Microsoft 365 Apps for enterprise installations.
- Identify how to prevent users from installing Microsoft 365 Apps for enterprise.
- Install and configure Microsoft 365 Apps for enterprise with the Office Deployment Tool.
- Deploy Microsoft 365 Apps for enterprise using Group Policy.
- Describe how to manage Microsoft 365 Apps for enterprise updates.

Module 4: Office 365 Overview

This module examines the primary features and functionality of the key Microsoft 365 services, including Exchange Online, SharePoint Online, Teams, Power Apps, Power Automate, Power BI, and Power Virtual Agents. This module also introduces you additional Microsoft 365 resources and provides an introduction to device management using Microsoft Intune, security baselines, and conditional access.

Lessons

- Exchange Online Overview
- SharePoint Online Overview
- Teams Overview
- Power Platform Overview
- Power Apps Overview
- Power Automate Overview
- Power BI Overview
- Power Virtual Agents Overview
- Additional Resources Overview
- Device Management Overview

Lab: Reviewing Office 365 Functionality

- Review Key Features of Exchange Online
- Review Key Features of SharePoint Online
- Create a Ticketing System in SharePoint
- Review Key Features of Microsoft Teams
- Explore the Power Platform Admin Center
- Create a Power App from a SharePoint data source
- Create a Power App from scratch
- Create a flow using Power Automate
- Create a DLP Policy using Power Automate
- Build a Power BI report and dashboard

After completing this module, delegates will be able to:

- Describe the most common recipient types are available in Exchange Online.
- Manage anti-malware and anti-spam policies in Exchange Online.
- Plan your organization's disaster recovery needs related to company and user emails.
- Determine retention tags and policies that will help you manage your organization’s email lifecycle.
- Describe migration and coexistence strategies and understand the differences between them.
- Select the right mail migration strategy for your organization.
- Determine when you want to change the DNS MX record for a domain in an Office 365 migration.
- Describe the different ways to migrate mailboxes to Office 365 in a hybrid Exchange environment.
- Determine the permission levels that your organization should use in SharePoint Online.
- Describe the levels of encryption for data at rest and data in transit within SharePoint Online.
- Describe the SharePoint Online options for maintaining and recovering content in an intranet.
- Describe the different options that provide anti-malware protection in SharePoint Online.
- Describe basic Teams functionality and the infrastructure that supports its goals.
- Describe how Teams compares to the other collaboration apps in Office 365.
- Manage user licenses in the Office 365 Admin Center and PowerShell to provide Teams access.
- Describe the functionality provided by Guess access in Microsoft Teams.
- Describe audio conferencing functionality that is available in Microsoft Teams.
- Manage user settings for audio conferencing.
- Implement phone systems in Microsoft Teams.
- Identify the components that make up the Power Platform product family.
- Describe the basic features of the Power Platform Admin center.
- Describe what Power Apps are, including their business impact and primary components.
- Describe how Power Apps connect to data sources.
- Create a basic Power App.
- Test and monitor a Power App.

- Run a Power App.
- Describe the Power Apps security structure.
- Build and run a basic workflow using Power Automate.
- Administer Power Automate.
- Build and share a basic Power BI report and dashboard.
- Administer Power BI.
- Explain what Power Virtual Agents are and how they empower teams to easily create powerful bots.
- Describe key features of Power Virtual Agents.
- Describe how device management enables organizations to protect and secure their resources and data.
- Describe how organizations use Microsoft Intune to secure proprietary data.
- Manage security baselines to secure devices
- Use conditional access to manage devices and apps.

Module 5: Configuring Microsoft 365 Clients

This module introduces you to the Microsoft 365 clients, including mobile clients and clients working offline. This module also examines how to configure Office client connectivity to Microsoft 365, including automatic client configuration, DNS records required for automatic client configuration, configuring Outlook clients, configuring MFA, and troubleshooting client connectivity.

Lessons

- Microsoft 365 Client Overview
- Configuring Office Client Connectivity to Microsoft 365

After completing this module, delegates will be able to:

- Identify the client packages supported by Microsoft 365.
- Identify the mobile clients supported by Microsoft 365.
- Identify the Microsoft 365 features that are available for each mobile client platform.
- Compare Office Online, Microsoft 365 Apps for enterprise, and Office 2016 Professional Plus.
- Work with Office Online apps.
- Describe how Outlook utilizes Autodiscover to initially connect an Outlook client to Exchange Online.
- Identify the DNS records needed for Outlook to locate the services in Office 365 using Autodiscover.
- Describe the connectivity protocols that enable Outlook to connect to Office 365.
- Describe how MFA increases security by adding an extra layer of user verification.

Module 6: Capturing User-Driven Data
This module examines how to capture user-driven data using Office Telemetry and Workplace Analytics.

Lessons

- Configuring Office Telemetry
- Configuring Workplace Analytics

After completing this module, delegates will be able to:

- Identify the five components of the Office Telemetry Dashboard.
- Describe the typical deployment requirements and issues that you might encounter when deployment Off.
- Describe the types of data collected by the Office Telemetry Agent.
- Install and configure Office Telemetry.
- Describe how Workplace Analytics can help organizations.
- Describe how organizations can use Workplace Analytics.
- Configure Workplace Analytics.
- Enroll devices in Workplace Analytics.
- Assess readiness using Workplace Analytics.

Module 7: Planning and Implementing Identity Synchronization
This module provides an in-depth examination of Microsoft 365 Identity synchronization, with a focus on Azure Active Directory Connect. You will learn how to plan for and implement Azure AD Connect and, how to manage synchronized identities, and how to implement password management in Microsoft 365 using multi-factor authentication and self-service password management.

Lessons

- Introduction to Identity Synchronization
- Planning for Azure AD Connect
- Implementing Azure AD Connect
- Managing Synchronized Identities
- Password Management in Microsoft 365

Lab: Manage Identities

- Prepare for Identity Synchronization
- Implement Identity Synchronization
- Implement Password Management

After completing this module, delegates will be able to:

- Describe the Microsoft 365 authentication options.
- Explain directory synchronization.
- Provide an overview of Azure AD Connect.
- Plan directory synchronization to synchronize your on-premises Active Directory objects to Azure AD.
- Plan an Azure AD Connect implementation.
- Plan for Azure AD Connect in a multi-forest scenario.
- Configure Azure AD Connect Prerequisites.
- Set up Azure AD Connect.
- Describe Azure AD Connect Health.
- Perform tasks to ensure users synchronize efficiently and successfully deploy Azure AD Connect.
- Manage groups with directory synchronization.
- Use Azure AD Connect Sync Security Groups to delegate control in Azure AD Connect to other users.
- Troubleshoot directory synchronization using a variety of troubleshooting tasks and tools.
- Describe the available password management features in Microsoft 365.

Module 8: Implementing Application and External Access

This module provides a comprehensive look at implementing application and external access. You will learn how to add and manage applications in Azure Active Directory, including how to configure multi-tenant applications. You will then examine how to configure Azure AD Application Proxy, including how to install and register a connector and how to publish an on-premises app for remote access. Finally, you will examine how to design and manage solutions for external access. This includes licensing guidance for Azure AD B2B collaboration, creating a collaborative user, and troubleshooting a B2B collaboration.

Lessons

- Implementing Applications in Azure AD
- Configuring Azure AD App Proxy
- Solutions for External Access

After completing this module, delegates will be able to:

- Register an application or service within your Azure AD tenant.
- Update an application within the Azure AD consent framework.
- Modify the configuration of a single-tenant application to make it a multi-tenant application.
- Remove an application's registration from your Azure AD tenant.
- Describe the benefits of Azure AD Application Proxy and how it works.
- Identify Azure AD application proxy prerequisites.
- Install and register a connector and verify that it installed correctly.
- Publish an on-premises app for remote access and test the published app to verify that it functions.
- Manage External Access with Azure AD B2B collaboration.
- Explain the difference between Microsoft 365 external access and Azure AD B2B collaboration.
- Explain the attributes of a collaborative User.
- Demonstrate Azure B2B Collaboration.
- Manage external access and guest access using Microsoft Teams.
- Manage customer lockbox requests.

Exam Details

This course leads to the MS-100 Microsoft 365 Identity & Services exam, which forms part of the Microsoft Certified: Enterprise Administrator Expert certification.

Microsoft 365 Mobility & Security

Course Code	MS101
Duration	5 days

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, Advanced Threat 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 the Security Dashboard and Advanced Threat Analytics to stay ahead of potential security breaches.

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, Information Rights Management, Secure Multipurpose Internet Mail Extension (S/MIME), Office 365 message encryption, and data loss prevention (DLP). You will then delve deeper into archiving and retention, paying particular attention to in-place records management in SharePoint, archiving and retention in Exchange, and Retention policies in the Security and Compliance Center.

Now that you understand the key aspects of data governance, you will examine how to implement them, including the building of ethical walls in Exchange Online, creating DLP policies from built-in templates, creating custom DLP policies, creating DLP policies to protect documents, and creating policy tips. You will then focus on managing data governance in Microsoft 365, including managing retention in email, troubleshooting retention policies and policy tips that fail, as well as troubleshooting sensitive data. You will then learn how to implement Azure Information Protection and Windows Information Protection. You will conclude this section by learning how to manage search and investigation, including searching for content in the Security and Compliance Center, auditing log investigations, and managing advanced eDiscovery.

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 10 devices for co-management. You will learn how to transition from Configuration Manager to Intune, and you will be introduced to the Microsoft Store for Business and Mobile Application Management. At this point, you will transition from planning to implementing device management; specifically, your Windows 10 deployment strategy. This includes learning how to implement Windows Autopilot, Windows Analytics, and Mobile Device Management (MDM). When examining MDM, you will learn how to deploy it, how to enrol devices to MDM, and how to manage device compliance.

Audience

This course is designed for persons who are aspiring to the Microsoft 365 Enterprise Admin role and have completed one of the Microsoft 365 role-based administrator certification paths.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Microsoft 365 Security Metrics
- Microsoft 365 Security Services
- Microsoft 365 Threat Intelligence
- Data Governance in Microsoft 365
- Archiving and Retention in Office 365
- Data Governance in Microsoft 365 Intelligence
- Search and Investigations
- Device Management
- Windows 10 Deployment Strategies
- Mobile Device Management

Prerequisites

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

Course Contents

Module 1: Introduction to Microsoft 365 Security Metrics
In this module, 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, including the Zero Trust approach. You will be introduced to the Microsoft Secure Score, Privileged Identity Management, as well as to Azure Active Directory Identity Protection.

Lessons

- Threat Vectors and Data Breaches
- The Zero Trust Model
- Security Solutions in Microsoft 365
- Introduction to Microsoft Secure Score
- Privileged Identity Management
- Introduction to Azure Active Directory Identity Protection

Lab: Tenant Setup and PIM

- Initialize your Microsoft 365 Tenant
- PIM Resource Workflows

After completing this module, delegates will be able to:

- Describe several 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.
- Describe the Zero Trust approach to security in Microsoft 365.
- Describe the components of Zero Trust security.
- Describe and five steps to implementing a Zero Trust model in your organization.
- Explain Zero Trust networking.
- List the types of threats that can be avoided by using EOP and Office 365 ATP.
- Describe how Microsoft 365 Threat Intelligence can be benefit your organization.
- Monitor your organization through auditing and alerts.
- Describe how ASM enhances visibility and control over your tenant through three core areas.
- Describe the benefits of Secure Score and what kind of services can be analyzed.
- Describe how to collect data using the Secure Score API.
- Know where to identify actions that will increase your security by mitigating risks.
- Explain how to determine the threats each action will mitigate and the impact it has on use.
- Explain Privileged Identity Management (PIM) in Azure administration.
- Configure PIM for use in your organization.
- Audit PIM roles.
- Explain Microsoft Identity Manager.
- Explain Privileged Access Management in Microsoft 365.
- Describe Azure Identity Protection and what kind of identities can be protected.
- Understand how to enable Azure Identity Protection.
- Know how to identify vulnerabilities and risk events.
- Plan your investigation in protecting cloud-based identities.
- Plan how to protect your Azure Active Directory environment from security breaches.

Module 2: Managing Your Microsoft 365 Security Services

This module examines how to manage the Microsoft 365 security services, including Exchange Online Protection, Advanced Threat Protection, Safe Attachments, and Safe Links. You will be introduced to the various reports that monitor your security health.

Lessons

- Introduction to Exchange Online Protection
- Introduction to Advanced Threat Protection
- Managing Safe Attachments
- Managing Safe Links
- Monitoring and Reports

Lab: Manage Microsoft 365 Security Services

- Implement a Safe Attachments policy
- Implement a Safe Links policy

After completing this module, delegates will be able to:

- Describe the anti-malware pipeline as email is analyzed by Exchange Online Protection.
- List several mechanisms used to filter spam and malware.
- Describe additional solutions to protect against phishing and spoofing.
- Describe the benefits of the Spoof Intelligence feature.
- Describe how Safe Attachments is used to block zero-day malware in email attachments and documents.
- Describe how Safe Links protect users from malicious URLs embedded in email and documents.
- Create and modify a Safe Attachments policy in the Security & Compliance Center.
- Create a Safe Attachments policy by using Windows PowerShell.
- Configure a Safe Attachments policy to take certain actions.
- Understand how a transport rule can be used to disable the Safe Attachments functionality.
- Describe the end-user experience when an email attachment is scanned and found to be malicious.
- Create and modify a Safe Links policy in the Security & Compliance Center.
- Create a Safe Links policy by using Windows PowerShell.
- Understand how a transport rule can be used to disable the Safe Links functionality.
- Describe the end-user experience when Safe Links identifies a link to a malicious website or file.
- Describe how reports provide visibility into how EOP and ATP is protecting your organization.
- Understand where to access reports generated by EOP and ATP.
- Understand how to access detailed information from reports generated by EOP and ATP.

Module 3: Microsoft 365 Threat Intelligence

In this module, you will then transition from security services to threat intelligence; specifically, using the Security Dashboard and Advanced Threat Analytics to stay ahead of potential security breaches.

Lessons

- Overview of Microsoft 365 Threat Intelligence
- Using the Security Dashboard
- Configuring Advanced Threat Analytics
- Implementing Your Cloud Application Security

Lab: Implement Threat Intelligence

- Conduct a Spear Phishing attack using the Attack Simulator
- Conduct Password attacks using the Attack Simulator
- Prepare for Alert Policies
- Implement a Mailbox Permission Alert
- Implement a SharePoint Permission Alert
- Test the Default eDiscovery Alert

After completing this module, delegates will be able to:

- Understand how threat intelligence is powered by the Microsoft Intelligent Security Graph.
- Describe how the threat dashboard can benefit C-level security officers.
- Understand how Threat Explorer can be used to investigate threats and help to protect your tenant.
- Describe how the Security Dashboard displays top risks, global trends, and protection quality.
- Describe what Advanced Thread Analytics (ATA) is and what requirements are needed to deploy it.
- Configure Advanced Threat Analytics.
- Manage the ATA services.
- Describe Cloud App Security.
- Explain how to deploy Cloud App Security.
- Control your Cloud Apps with Policies.
- Troubleshoot Cloud App Security.

Module 4: Introduction to Data Governance in Microsoft 365
This module examines 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, Information Rights Management, Secure Multipurpose Internet Mail Extension (S/MIME), Office 365 message encryption, and data loss prevention (DLP).

Lessons

- Introduction to Archiving in Microsoft 365
- Introduction to Retention in Microsoft 365
- Introduction to Information Rights Management
- Introduction to Secure Multipurpose Internet Mail Extension
- Introduction to Office 365 Message Encryption
- Introduction to Data Loss Prevention

Lab: Implement Message Encryption and IRM

- Configure Microsoft 365 Message Encryption
- Validate Information Rights Management

After completing this module, delegates will be able to:

- Understand Data Governance in Microsoft 365.
- Describe the difference between In-Place Archive and Records Management.
- Explain how data is archived in Exchange.
- Recognize the benefits of In Place Records Management in SharePoint.
- Explain the difference between Message Records Management (MRM) in Exchange and Retention in SCC.
- Understand how MRM works in Exchange.
- List the types of retention tags that can be applied to mailboxes.
- Know the different Microsoft 365 Encryption Options.
- Understand how IRM can be used in Exchange.
- Configure IRM protection for Exchange mails.
- Explain how IRM can be used in SharePoint.
- Apply IRM protection to SharePoint documents.
- Tell the differences between IRM protection and AIP classification.
- Describe the use of S/MIME.
- Explain what digital signatures are.
- Apply a digital signature to a message.
- Understand how message encryption works.
- Perform encryption on a message.
- Accomplish decryption of a message.
- Understand the co-operation of signing and encryption simultaneously.
- Tell what triple-wrapped messages are.
- Describe when you can use Office 365 Message Encryption.
- Explain how Office 365 Message Encryption works.
- Describe Data Loss Prevention (DLP).
- Understand what sensitive information and search patterns are that DLP is using.
- Know what a DLP policy is and what it contains.
- Recognize how actions and conditions work together for DLP.
- Express how actions contain functions to send emails on matches.
- Show policy tips to the users if a DLP rule applies.
- Use policy templates to implement DLP policies for commonly used information.
- Explain document finger.
- Understand how to use DLP to protect documents in Windows Server FCI.

Module 5: Archiving and Retention in Microsoft 365

This module delves deeper into archiving and retention, paying particular attention to in-place records management in SharePoint, archiving and retention in Exchange, and Retention policies in the Security and Compliance Center.

Lessons

- In-Place Records Management in SharePoint
- Archiving and Retention in Exchange
- Retention Policies in the SCC

Lab: Implement Archiving and Retention

- Initialize Compliance
- Configure Retention Tags and Policies

After completing this module, delegates will be able to:

- Understand the process of records management.
- Create a file plan for your organization.
- Describe two methods for converting active docs to records.
- Describe the benefits of In-Place Records Management.
- Configure of In-Place Records Management for your organization.
- Enable and disable In-Place Archiving.
- Create useful retention tags.
- Create retention policies to group retention tags.
- Assign retention policies to mailboxes.
- Allocate permissions and scripts to export and import retention tags.
- Export all retention policies and tags from an organization.
- Import all retention policies and tags to an organization.
- Explain how a retention policy works.
- Create a retention policy.
- Manage retention policy settings.

Module 6: Implementing Data Governance in Microsoft 365 Intelligence

This module examines how to implement the key aspects of data governance, including the building of ethical walls in Exchange Online, creating DLP policies from built-in templates, creating custom DLP policies, creating DLP policies to protect documents, and creating policy tips.

Lessons

- Evaluating Your Compliance Readiness
- Implementing Compliance Center Solutions
- Building Ethical Walls in Exchange Online
- Creating a Simple DLP Policy from a Built-in Template
- Creating a Custom DLP Policy
- Creating a DLP Policy to Protect Documents
- Working with Policy Tips

Lab: Implement DLP Policies

- Manage DLP Policies
- Test MRM and DLP Policies

After completing this module, delegates will be able to:

- Describe the Microsoft 365 Compliance Center and how to access it.
- Describe the purpose and function of Compliance score.
- Explain the components of how an organization's Compliance score is determined.
- Explain how assessments are used to formulate compliance scores.
- Explain how Microsoft 365 helps address Global Data Protection Regulation.
- Describe insider risk management functionality in Microsoft 365.
- Configure insider risk management policies.
- Configure insider risk management policies.
- Explain the communication compliance capabilities in Microsoft 365.
- Describe what an ethical wall in Exchange is and how it works.
- Explain how to create an ethical wall in Exchange.
- Identify best practices for building and working with ethical walls in Exchange.
- Understand the different built-in templates for a DLP policies.
- Determine how to choose the correct locations for a DLP policy.
- Configure the correct rules for protecting content.
- Enable and review the DLP policy correctly.
- Describe how to modify existing rules of DLP policies.
- Explain how to add and modify custom conditions and action to a DLP rule.
- Describe how to change user notifications and policy tips.
- Configure the user override option to a DLP rule.
- Explain how incident reports are sent by a DLP rule violation.
- Describe how to work with managed properties for DLP policies.
- Explain how SharePoint Online creates crawled properties from documents.
- Describe how to create a managed property from a crawled property in SharePoint Online.
- Explain how to create a DLP policy with rules that apply to managed properties via PowerShell.
- Describe the user experience when a user creates an email or site containing sensitive information.
- Explain the behaviour in Office apps when a user enters sensitive information.
- Implementing Windows Information Protection

Module 7: Managing Data Governance in Microsoft 365

This module focuses on managing data governance in Microsoft 365, including managing retention in email, troubleshooting retention policies and policy tips that fail, as well as troubleshooting sensitive data. You will then learn how to implement Azure Information Protection and Windows Information Protection.

Lessons

- Managing Retention in Email
- Troubleshooting Data Governance
- Implementing Azure Information Protection
- Implementing Advanced Features of AIP
- Implementing Windows Information Protection

Lab: Implement AIP and WIP

- Implement Azure Information Protection
- Implement Windows Information Protection

After completing this module, delegates will be able to:

- Determine when and how to use retention tags in mailboxes.
- Assign retention policy to an email folder.
- Add optional retention policies to email messages and folders.
- Remove a retention policy from an email message.
- Explain how the retention age of elements is calculated.
- Repair retention policies that do not run as expected.
- Understand how to systematically troubleshoot when a retention policy appears to fail.
- Perform policy tests in test mode with policy tips.
- Describe how to monitor DLP policies through message tracking.
- Describe the required planning steps to use AIP in your company.
- Configure and customize labels.
- Create policies to publish labels.
- Plan a Deployment of the Azure Information Protection client.
- Configure the advance AIP service settings for Rights Management Services (RMS) templates.
- Implement automatic and recommended labelling.
- Activate the Super User feature for administrative tasks.
- Create your tenant key for encryption.
- Deploy the AIP scanner for on-premises labelling.
- Plan RMS connector deployment to connect on-premises servers.
- Describe WIP and what it is used for.
- Plan a deployment of WIP policies.
- Implement WIP policies with Intune and SCCM.
- Implement WIP policies in Windows desktop apps.

Module 8: Managing Search and Investigations
This module concludes this section on data governance by examining how to manage search and investigation, including searching for content in the Security and Compliance Center, auditing log investigations, and managing advanced eDiscovery.

Lessons

- Searching for Content in the Security and Compliance Center
- Auditing Log Investigations
- Managing Advanced eDiscovery

Lab: Manage Search and Investigations

- Implement a Data Subject Request
- Investigate Your Microsoft 365 Data

After completing this module, delegates will be able to:

- Describe how to use content search.
- Design your content search.
- Configure search permission filtering.
- Explain how to search for third-party data.
- Describe when to use scripts for advanced searches.
- Describe what the audit log is and the permissions that are necessary to search the Office 365 audit.
- Configure Audit Policies.
- Enter criteria for searching the audit log.
- View, sort, and filter search results.
- Export search results to a CSV file.
- Search the unified audit log by using Windows PowerShell.
- Describe Advanced eDiscovery.
- Configure permissions for users in Advanced eDiscovery.
- Create Cases in Advanced eDiscovery.
- Search and prepare data for Advanced eDiscovery.

Module 9: Planning for Device Management

This module provides an in-depth examination of Microsoft 365 Device management. You will begin by planning for various aspects of device management, including preparing your Windows 10 devices for co-management. You will learn how to transition from Configuration Manager to Microsoft Intune, and you will be introduced to the Microsoft Store for Business and Mobile Application Management.

Lessons

- Introduction to Co-management
- Preparing Your Windows 10 Devices for Co-management
- Transitioning from Configuration Manager to Intune
- Introduction to Microsoft Store for Business
- Planning for Mobile Application Management

Lab: Implement the Microsoft Store for Business

- Configure the Microsoft Store for Business.
- Manage the Microsoft Store for Business.

After completing this module, delegates will be able to:

- Describe the benefits of Co-management.
- Plan your organization's Co-management Strategy.
- Describe the main features of Configuration Manager.
- Describe how Azure Active Directory enables co-management.
- Identify the prerequisites for using Co-management.
- Configure Configuration Manager for Co-management.
- Enroll Windows 10 Devices to Intune.
- Modify your co-management settings.
- Transfer workloads to Intune.
- Monitor your co-management solution.
- Check compliance for co-managed devices.
- Describe the feature and benefits of the Microsoft Store for Business.
- Configure the Microsoft Store for Business.
- Manage settings for the Microsoft Store for Business.

Module 10: Planning Your Windows 10 Deployment Strategy
This module focuses on planning your Windows 10 deployment strategy, including how to implement Windows Autopilot and Windows Analytics, and planning your Windows 10 subscription activation service.

Lessons

- Windows 10 Deployment Scenarios
- Implementing and Managing Windows Autopilot
- Planning Your Windows 10 Subscription Activation Strategy
- Resolving Windows 10 Upgrade Errors
- Introduction to Windows Analytics

After completing this module, delegates will be able to:

- Plan for Windows as a Service.
- Plan a Modern Deployment.
- Plan a Dynamic Deployment.
- Plan a Traditional Deployment.
- Describe Windows Autopilot requirements.
- Configure Autopilot.
- Create and Assign an Autopilot profile.
- Deploy and validate Autopilot.
- Describe Autopilot Self-deployments, White Glove deployments, and User-drive deployments.
- Deploy BitLocker Encryption for Autopiloted Devices.
- Understand Windows 10 Enterprise E3 in CSP.
- Configure VDA for Subscription Activation.
- Deploy Windows 10 Enterprise licenses.
- Describe common fixes for Windows 10 upgrade errors.
- Use SetupDiag.
- Troubleshooting upgrade errors.
- Describe Windows error reporting.
- Understand the upgrade error codes and resolution procedure.
- Describe Windows Analytics.
- Describe Device Health.
- Describe Update Compliance.
- Determine Upgrade Readiness.

Module 11: Implementing Mobile Device Management
This module focuses on Mobile Device Management (MDM). You will learn how to deploy it, how to enrol devices to MDM, and how to manage device compliance.

Lessons

- Planning Mobile Device Management
- Deploying Mobile Device Management
- Enrolling Devices to MDM
- Managing Device Compliance

Lab: Manage Devices with Intune

- Enable Device Management
- Configure Azure AD for Intune
- Create Intune Policies
- Enroll a Windows 10 Device
- Manage and Monitor a Device in Intune

After completing this module, delegates will be able to:

- Manage devices with MDM.
- Compare MDM for Office 365 and Intune.
- Understand policy settings for mobile devices.
- Control Email and Document Access.
- Activate Mobile Device Management Services.
- Deploy Mobile Device Management.
- Configure Domains for MDM.
- Configure an APNs Certificate for iOS devices.
- Manage Device Security Policies.
- Define a Corporate Device Enrolment Policy.
- Enroll devices to MDM.
- Understand the Apple Device Enrolment Program.
- Understand Enrolment Rules.
- Configure a Device Enrolment Manager Role.
- Describe Multi-factor Authentication considerations.
- Plan for device compliance.
- Configure conditional users and groups.
- Create Conditional Access policies.
- Monitor enrolled device

Exam Details

This course leads to the MS-101 Microsoft 365 Mobility & Security exam, which forms part of the Microsoft Certified: Enterprise Administrator Expert certification.

Microsoft 365 Messaging

Course Code	MS203
Duration	5 days

Overview

This course examines the key elements of Microsoft 365 messaging administration, including message transport and mail flow, messaging security, hygiene, and compliance, messaging infrastructure, and hybrid messaging. This course is designed for IT Professionals who deploy and manage the messaging infrastructure for Microsoft 365 in their organization.

Audience

The Messaging Administrator deploys, configures, manages, and troubleshoots recipients, permissions, mail protection, mail flow, and public folders in both on-premises and cloud enterprise environments. Responsibilities include managing message hygiene, messaging infrastructure, and hybrid configuration and migration. To implement a secure hybrid topology that meets the business needs of a modern organization, the Messaging Administrator must collaborate with the Security Administrator and Microsoft 365 Enterprise Administrator. The Messaging Administrator should have a working knowledge of authentication types, licensing, and integration with Microsoft 365 applications.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Configure and manage the transport pipeline.
- Manage and troubleshoot mail flow and transport issues.
- Manage message hygiene and compliance.
- Manage authentication for messaging.
- Configure organizational settings and sharing.
- Manage mobile devices.
- Manage role-based permissions.
- Create and manage recipient objects and resources.
- Plan, implement, and troubleshoot public folders.
- Plan a hybrid environment.
- Perform mailbox migrations.
- Deploy and troubleshoot a hybrid environment.

Prerequisites

This course is designed for persons who are aspiring to the Microsoft 365 Messaging Administrator role.

Course Contents

Module 1: Managing the Transport Pipeline
In this module, you will learn about the different transport components of Exchange, how the message routing works, and how to configure the message flow for your organization. You will examine the tasks that messaging administrators must complete to configure message transport. You will review the message transport options and learn how to configure domains and connectors and how to implement an approval workflow for messaging. You will also learn how to manage transport rules, which are a very powerful configuration to control the message flow in your organization.

Lessons

- Overview of Transport Services
- Configuring Message Transport
- Managing Transport Rules

Lab: Configure Message Transport

- Create Connectors

After completing this module, delegates will be able to:

- Describe the transport components of Exchange.
- Plan an effective message routing for your organization.
- Modify message flow for your organization.
- Describe which transport agents exist and what they do.
- Configure the different transport options.
- Plan and set up domains for your organizations.
- Understand how receive and send connectors work.
- Describe how message moderation for different recipients work.
- Understand what transport rules are.
- Describe how transport rules are working.
- Configure custom transport rules.
- Describe how transport rules can be used for data loss prevention.

Module 2: Managing and Troubleshooting Mail Flow

In this module, you will examine the components of mail flow, and you will learn how to manage your mail flow, which is a crucial task for every Exchange administrator. You will study the differences between managing mail flow in Exchange Online, Exchange Server, and Exchange Hybrid deployments. From managing mail flow, you will transition to troubleshooting mail flow issues such as emails not being routed correctly in or outside your organization, or when secure connections cannot be established successfully. You will learn about the tools Microsoft provides to help you find the root cause of your issues and fix your mail flow. You will then transition from troubleshooting mail flow to troubleshooting transport issues, such as network-based issues, connector and agent issues, and architectural issues, as well as how to troubleshoot in coexistence. Finally, you will learn how to check event, protocol, and tracking logs when all troubleshooting for service availability and message transport has finished and an issue still persists, or if you must find historical data about issues in the past.

Lessons

- Managing Mail Flow
- Troubleshooting Mail Flow
- Troubleshooting Transport Issues
- Troubleshooting with Logs

Lab: Conditional Mail Routing

- Create Mail Flow Rules

After completing this module, delegates will be able to:

- Manage mail flow in organizations.
- Understand mail flow for Exchange Servers.
- Manage mail flow for Exchange Online.
- Describe and manage mail flow in hybrid environments.
- Understand how to troubleshoot SMTP mail flow issues.
- Describe how to troubleshoot issues with a shared namespace.
- Describe how to troubleshoot encryption issues with TLS.
- Perform troubleshooting for network-based issues.
- Describe troubleshooting procedures for connector and agent issues.
- Plan troubleshooting for architectural issues.
- Understand how to perform troubleshooting in coexistence.
- Create searches for the message tracking log.
- Describe how to troubleshoot using the protocol logs.
- Understand how to work with the event logging for Exchange.

Module 3: Managing Message Hygiene

In this module, you will learn about Microsoft Exchange Online Protection (EOP) features and functionality. You will also learn how to plan messaging routing for this service, which provides anti-malware and anti-spam policies that protect your organization against spam and malware and safeguards your organization from messaging-policy violations. You will then review the anti-malware and anti-spam protection that Exchange Server and Online Protection provide, and you will learn how to configure SPAM and malware filters, policies, and settings to provide protection for your users. You will conclude the module by examining Advanced Threat Protection (ATP) and how it extends the protection provided by EOP by filtering targeted attacks that could pass through EOP's line of defenses, including advanced threats such as zero-day attacks in email attachments and Office documents and time-of-click protection against malicious URLs. You will learn how Microsoft 365 ATP protects users from advanced threats through features such as safe attachments and safe links, and how it generates reports which provide administrators with insight into attacks targeting their tenants through email.

Lessons

- Planning for Message Hygiene
- Managing Anti-Malware and Anti-Spam Policies
- Managing Advanced Threat Protection

Lab: Managing Messaging Hygiene

- Create Hygiene Filters

After completing this module, delegates will be able to:

- Explain the use and features of Exchange Online Protection.
- Plan message routing for Exchange Online Protection.
- Investigate the available EOP reports and logs.
- Understand the different message header fields relevant for spam and spoofing protection.
- Configure anti-spam and anti-malware filters in Exchange Server.
- Using additional features for outbound spam filtering and quarantine.
- Implementing protection features against phishing and spoofing.
- Create transport rules for custom requirements.
- Describe the features of Advanced Threat Protection.
- Describe the protection provided by Safe Attachment and Safe Links policies.
- Understand the spoof intelligence features.
- Know how ATP anti-phishing policies work.

Module 4: Managing Compliance

This module begins by describing the different compliance features in the Security & Compliance Center (SCC) that messaging administrators can use to comply with legal and regulatory requirements. This module supports compliance in Exchange by examining the compliance features available in the Exchange Admin Center for Exchange Server and hybrid deployments. Because of the complex retention requirements of modern messaging environments, this module focuses on how archiving is performed with Exchange so that you can provide an efficient and compliant environment to your users. You will also examine how additional archive storage is provided to your users, how messages are automatically processed and archived, and how audit logging in Exchange that provides information about administrator, delegate, and user actions in user mailboxes and your Exchange organization. Finally, because organizations must adhere to legal discovery requirements (related to organizational policy, compliance, or lawsuits), you will examine how eDiscovery for Microsoft Exchange can help you perform discovery searches for relevant content within mailboxes.

Lessons

- Messaging Compliance in the SCC
- Messaging Compliance in Exchange
- Managing Exchange Online Archiving and Auditing
- Managing Content Search

After completing this module, delegates will be able to:

- Describe different policy and compliance features for messaging.
- Evaluate the different roles in the Security & Compliance Center.
- Plan retention policies for Exchange Online mailboxes.
- Configure data loss prevention (DLP) policies for data in Microsoft 365.
- Create message traces to understand the mail flow in your Exchange Online organization.
- Describe litigation and in-place holds in Exchange Server.
- Plan retention and deletion with Message Records Management (MRM).
- Protect your mail flow with data loss prevention policies in Exchange Server.
- Investigate the message tracking log in your Exchange organization.
- Describe what in-place archiving is and how it works.
- Understand the differences between journaling and archiving.
- Know what the mailbox and administrator audit logs are used for.
- Understand content searches to search for messages in your organization.
- Describe eDiscovery cases and in-place eDiscovery for Exchange.
- Manage Advanced eDiscovery cases in the Security & Compliance Center.

Module 5: Managing Organizational Settings
This module begins with an examination on how to manage authentication for messaging. This module focuses on how to ensure that user accounts are well protected and secure, and how to deploy multiple security features that do not introduce unnecessary complexity in users' everyday work, which can result in lower business productivity and new security risks. You will then transition from messaging authentication to organizational settings, where you will learn how to configure settings that apply to the entire organization or to many users in the organization. Finally, you will examine how to configure organizational sharing.

Lessons

- Managing Authentication for Messaging
- Configuring Organizational Settings
- Configuring Organizational Sharing

After completing this module, delegates will be able to:

- Configure password policy options.
- Configure self-service password management.
- Implement multi-factor authentication.
- Plan password policies.
- Configure workload policies and throttling.
- Configure quota configurations.
- Configure Exchange Server and Skype for Business integration.
- Deploy Office 365 add-ins.
- Provide an overview of Exchange federated delegation sharing features.
- Describe federated sharing components.
- Explain considerations for designing and implementing federation trusts and certificates.
- Implement organization relationships.
- Implement sharing policies.

Module 6: Managing Mobile Devices
In this module, you will begin by examining Mobile Device Management in Microsoft 365, as well as how Exchange ActiveSync and mobile device mailbox policies support this effort. You will then examine how to manage and troubleshoot mobile device access. This module then examines how to configure both access and infrastructure for mobile devices, understanding the implications of mobile device remote wipe, and learning about alternative methods for mobile device management.

Lessons

- Mobile Device Mailbox Policies
- Managing Mobile Device Access

Lab: Implement ActiveSync

- Implement Active Sync for single and multiple mailboxes

After completing this module, delegates will be able to:

- Describe how Exchange ActiveSync works.
- Configure mobile device mailbox policies.
- Understand Mobile Device Management in Microsoft 365.
- Configure access for mobile devices.
- Understand components of mobile device infrastructure.
- Tell how a mobile device remote wipe works.
- Describe alternatives for mobile device management.
- Troubleshoot mobile device access.

Module 7: Managing Role-Based Permissions

This module examines how messaging administrators manage role-based permissions, which is an essential task for any messaging administrator. Since Exchange Server and Exchange Online both use the Role Based Access Control (RBAC) permission model, this module examines the basics of RBAC management. The module concludes by examining how a messaging administrator must plan and configure permissions carefully so as not to put their environment or their entire Active Directory at risk.

Lessons

- Managing Admin Roles
- Managing User Roles
- Exchange Setup - RBAC and AD Split Permission

Lab: Manage Roles and Permission Policies

- Manage Roles and Permission Policies

After completing this module, delegates will be able to:

- Describe how RBAC is used to assign roles to users.
- Understand what management role group for administrative tasks are.
- Assign the built-in management roles for administration.
- Create custom management roles and assign them through role assignment policies to users.
- Troubleshoot RBAC management roles.
- Describe the built-in end-user roles.
- Configure role assignment policies.
- Create new custom roles and role assignment policies.
- Understand the differences between shared permissions and split permissions.
- Describe multi-forest permissions.
- Identify the differences between the permission models.

Module 8: Managing Recipient Objects and Resources
This module examines some of the most common tasks that messaging administrators perform - creating and configuring email recipients, lists, and resources. This module examines the different types of Exchange Server recipients, including how they differ from each other. The module then focuses on the various tasks that require you to create and manage Exchange recipients in Exchange, including user mailboxes, resource mailboxes, shared mailboxes, mail contacts, and mail users. You will also learn how to manage permissions for recipients, and how to create and manage groups.

Lessons

- Exchange Recipients
- Creating and Managing Exchange Recipients
- Managing Email Addresses, Lists, and Resources

Lab: Create Recipient Objects and Resources

- Create Exchange Recipients
- Create Groups

After completing this module, delegates will be able to:

- Describe the different recipient objects in Exchange.
- Describe resource mailboxes.
- Describe shared mailboxes.
- Describe linked mailboxes and site mailboxes.
- Describe groups.
- Create and manage Mailbox settings.
- Create and manage Resource and Shared mailboxes.
- Create and manage Mail contacts and mail users.
- Create and manage Recipient permissions.
- Create and manage Groups.
- Describe address lists.
- Explain how to configure address lists.
- Describe address book policies.
- Explain how to configure offline address books.
- Describe email address policies.

Module 9: Managing Public Folders

In this module, you will learn about public folders in Exchange, review the planning considerations for deploying public folders, and discuss alternatives to public folders. You will also learn how to implement and manage public folder mailboxes, public folders, and public folder permissions, as well as how to create and manage mail-enabled public folders. The module concludes by examining how to monitor and troubleshoot Public Folder-related issues.

Lessons

- Planning the Public Folder Hierarchy
- Implementing and Managing Public Folders
- Troubleshooting Public Folders

Lab: Implement Public Folders

- Create Public Folders
- Manage Public Folders

After completing this module, delegates will be able to:

- Describe public folders in Exchange.
- Plan a public folder hierarchy.
- Plan public folder mailboxes.
- Explain public folder quotas.
- Evaluate alternatives to public folders.
- Describe considerations for implementing Public Folders.
- Deploy public folder mailboxes.
- Manage public folder permissions.
- Create and manage mail-enabled public folders.
- Monitor public folders.
- Troubleshoot public folders.
- Troubleshoot public folder access.

Module 10: Planning a Hybrid Environment

In this module you will examine the requirements necessary to implement a hybrid deployment, and you will learn about the features and components that are required when implementing a hybrid deployment. This module examines all planning aspects that are required before running the Hybrid Configuration Wizard. This includes the configuration options of the HCW, as well as the details on Organization Configuration Transfer (OCT) and the Hybrid Agent. The module concludes with a review of the mail flow options for a hybrid deployment.

Lessons

- Exchange Hybrid Deployment Requirements
- Planning to Run the Hybrid Configuration Wizard

Lab: Prepare Azure AD for Hybrid Synchronization

- Prepare Azure AD for Hybrid Synchronization

After completing this module, delegates will be able to:

- Describe connection options that are available for connecting on-premises Exchange to Microsoft 365.
- List and describe components of a hybrid deployment.
- Describe Azure Active Directory Connect (Azure AD Connect).
- Identify Microsoft 365 identity options for Exchange hybrid.
- Compare Exchange delegated federation vs. OAuth.
- Plan for Exchange Hybrid configuration.
- Describe Organization Configuration Transfer.
- Explain Exchange Modern Hybrid and Hybrid Agent.
- Plan mail flow options for a hybrid deployment.

Module 11: Performing Mailbox Migrations

This module examines the options that are available for migrating email to Exchange Online, such as performing a migration or using FastTrack to move mailboxes from your existing mail servers to Exchange Online. This module summarizes the migration and co-existence options and recommends when to use which option. The module then examines the requirements for running an IMAP migration, the migration options that are available, and the steps that are performed during a migration. The module then examines how to plan and perform both a cutover and staged migration. It compares each of these two migration approaches, and you will learn about the requirements, planning activities, and migration process for each option. The module concludes by examining important additional migration tasks, such as migrating a PST file and the considerations for a Public Folder migration.

Lessons

- Planning Mailbox Migrations
- Performing IMAP Migrations
- Performing Cutover and Staged Migrations
- Performing Advanced Migrations

After completing this module, delegates will be able to:

- Describe the migration and coexistence strategies with Exchange Online.
- Use FastTrack to move mailboxes.
- Describe the requirements for an IMAP migration and how it’s carried out.
- Move mailbox data using an IMAP migration.
- Describe the requirements for both cutover and staged migrations.
- Perform a migration and move mailboxes either with a cutover or staged migration.
- Import PST Files to Exchange Online mailboxes.
- Migrate Public Folders to Exchange Online.

Module 12: Deploying and Troubleshooting a Hybrid Environment

In this module you will learn the key areas to plan for regarding Edge Transport servers. You will then learn about the requirements and best practices to configure a hybrid deployment, which is the first step for your Exchange organization, regardless of whether you want to connect your Exchange on-premises and Exchange Online organizations for long-term coexistence or as part of a cloud migration strategy. In this module, you will then examine how to manage a hybrid deployment and implement advanced hybrid functionality. You will cover the features that require a successful hybrid deployment such as Public Folder coexistence or OneDrive for Business attachment storage for on-premises mailboxes. This module concludes with an introduction to troubleshooting techniques for a hybrid deployment. You will learn how to troubleshoot directory synchronization issues including pass-through authentication (PTA) and single sign-on, Exchange transport, and client access troubleshooting as well as mailbox replication service troubleshooting.

Lessons

- Deploying and Managing an Edge Transport Server
- Configuring a Hybrid Deployment using the HCW
- Implementing Advanced Hybrid Functionality
- Troubleshooting Hybrid Deployments

Lab: Deploy a Hybrid Environment

- Set Up your Hybrid Deployment
- Test your Hybrid Deployment

After completing this module, delegates will be able to:

- Describe the purpose and functionality of Edge Transport servers.
- Explain the infrastructure requirements for Edge Transport servers.
- Describe EdgeSync.
- Plan for message flow with an Edge Transport server.
- Describe the prerequisites to run the Office 365 Hybrid Configuration Wizard.
- Explain best practices for implementing a hybrid deployment.
- Manage a hybrid deployment.
- Describe when you must configure Public Folder coexistence with Office 365.
- Explain how to configure Oauth for a mixed Exchange environment.
- Describe how to configure OneDrive for Business attachments for on-premises mailboxes.
- Troubleshoot Directory synchronization.
- Troubleshoot Pass-Through Authentication and Single Sign-On.
- Troubleshoot Transport with Exchange Online.
- Troubleshoot Client Access in Coexistence.
- Troubleshoot Mailbox Replication Service.

Exam Details

This course leads to the MS-203 Microsoft 365 Messaging exam, which will earn you the Microsoft 365 Certified: Messaging Administrator Associate certification.

Microsoft 365 Security Administration

Course Code	MS500
Duration	4 days

Overview

In this course you will learn how to secure user access to your organization’s resources. The course covers user password protection, multi-factor authentication, how to enable Azure Identity Protection, how to setup and use Azure AD Connect, and introduces you to conditional access in Microsoft 365. You will learn about threat protection technologies that help protect your Microsoft 365 environment. Specifically, you will learn about threat vectors and Microsoft’s security solutions to mitigate threats. You will learn about Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and threat management. In the course you will learn about information protection technologies that help secure your Microsoft 365 environment. The course discusses information rights managed content, message encryption, as well as labels, policies and rules that support data loss prevention and information protection. Lastly, you will learn about archiving and retention in Microsoft 365 as well as data governance and how to conduct content searches and investigations. This course covers data retention policies and tags, in-place records management for SharePoint, email retention, and how to conduct content searches that support eDiscovery investigations.

Audience

The Microsoft 365 Security administrator collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and to ensures that the solutions comply with the policies and regulations of the organization. This role proactively secures Microsoft 365 enterprise environments. Responsibilities include responding to threats, implementing, managing and monitoring security and compliance solutions for the Microsoft 365 environment. They respond to incidents, investigations and enforcement of data governance. The Microsoft 365 Security administrator is familiar with Microsoft 365 workloads and hybrid environments. This role has strong skills and experience with identity protection, information protection, threat protection, security management and data governance.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Administer user and group access in Microsoft 365.
- Explain and manage Azure Identity Protection.
- Plan and implement Azure AD Connect.
- Manage synchronized user identities.
- Explain and use conditional access.
- Describe cyber-attack threat vectors.
- Explain security solutions for Microsoft 365.
- Use Microsoft Secure Score to evaluate and improve your security posture.
- Configure various advanced threat protection services for Microsoft 365.
- Plan for and deploy secure mobile devices.
- Implement information rights management.
- Secure messages in Office 365.
- Configure Data Loss Prevention policies.
- Deploy and manage Cloud App Security.
- Implement Windows information protection for devices.
- Plan and deploy a data archiving and retention system.
- Create and manage an eDiscovery investigation.
- Manage GDPR data subject requests.

Prerequisites

- Basic conceptual understanding of Microsoft Azure.
- Experience with Windows 10 devices.
- Experience with Office 365.
- Basic understanding of authorization and authentication.
- Basic understanding of computer networks.
- Working knowledge of managing mobile devices.

Course Contents

Module 1: User and Group Management
This module explains how to manage user accounts and groups in Microsoft 365. It introduces you to the Zero Trust concept as well as authentication. The module sets the foundation for the remainder of the course.

Lessons
Identity and Access Management concepts
The Zero Trust model
Plan your identity and authentication solution
User accounts and roles
Password Management

Lab: Initialize your tenant - users and groups
Set up your Microsoft 365 tenant
Manage users and groups

Lab: Password management
Configure Self-service password reset (SSPR) for user accounts in Azure AD
Deploy Azure AD Smart Lockout

After completing this module, delegates will be able to:
Create and manage user accounts.
Describe and use Microsoft 365 admin roles.
Plan for password policies and authentication.
Describe the concepts of Zero Trust security.
Explain the Zero Trust model.

Module 2: Identity Synchronization and Protection

This module explains concepts related to synchronizing identities for Microsoft 365. Specifically, it focuses on Azure AD Connect and managing directory synchronization to ensure the right people are connecting to your Microsoft 365 system.

Lessons

- Plan directory synchronization
- Configure and manage synchronized identities
- Azure AD Identity Protection

Lab: Implement Identity Synchronization

- Set up your organization for identity synchronization

After completing this module, delegates will be able to:

- Explain directory synchronization.
- Plan directory synchronization.
- Describe and use Azure AD Connect.
- Configure Azure AD Connect Prerequisites.
- Manage users and groups with directory synchronization.
- Describe Active Directory federation.
- Enable Azure Identity Protection

Module 3: Identity and Access Management

This module explains conditional access for Microsoft 365 and how it can be used to control access to resources in your organization. The module also explains Role Based Access Control (RBAC) and solutions for external access. We discuss identity governance as a concept and its components.

Lessons

- Application Management
- Identity Governance
- Manage device access
- Role Based Access Control (RBAC)
- Solutions for external access
- Privileged Identity Management

Lab: Use Conditional Access to enable MFA

- MFA Authentication Pilot (require MFA for specific apps)
- MFA Conditional Access (complete an MFA roll out)

Lab: Configure Privileged Identity Management

- Manage Azure resources
- Assign directory roles
- Activate and deactivate PIM roles
- Directory roles
- PIM resource workflows
- View audit history for Azure AD roles in PIM

After completing this module, delegates will be able to:

- Describe the concept of conditional access.
- Describe and use conditional access policies.
- Plan for device compliance.
- Configure conditional users and groups.
- Configure role-based access control.
- Describe the concepts of identity governance.
- Configure and use Privileged Identity Management.

Module 4: Security in Microsoft 365

This module explains the various cyber-attack threats that exist. It then introduces you to the Microsoft solutions used to mitigate those threats. The module finishes with an explanation of Microsoft Secure Score and how it can be used to evaluate and report your organizations security posture.

Lessons

- Threat vectors and data breaches
- Security strategy and principles
- Microsoft security solutions
- Secure Score

Lab: Use Microsoft Secure Score

- Improve your secure score in the Microsoft 365 Security Center

After completing this module, delegates will be able to:

- Describe several techniques attackers use to compromise user accounts through email.
- Describe techniques attackers use to gain control over resources.
- List the types of threats that can be avoided by using EOP and Microsoft Defender for Office 365.
- Describe the benefits of Secure Score and what kind of services can be analyzed.
- Describe how to use Secure Score to identify gaps in your current Microsoft 365 security posture.

Module 5: Threat Protection

This module explains the various threat protection technologies and services available for Microsoft 365. The module covers message protection through Exchange Online Protection, Microsoft Defender for Identity and Microsoft Defender for Endpoint.

Lessons

- Exchange Online Protection (EOP)
- Microsoft Defender for Office 365
- Manage Safe Attachments
- Manage Safe Links
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint

Lab: Manage Microsoft 365 Security Services

- Implement Microsoft Defender Policies

After completing this module, delegates will be able to:

- Describe the anti-malware pipeline as email is analyzed by Exchange Online Protection.
- Describe how Safe Attachments is used to block zero-day malware in email attachments and documents.
- Describe how Safe Links protect users from malicious URLs embedded in email and documents that point.
- Configure Microsoft Defender for Identity.
- Configure Microsoft Defender for Endpoint.

Module 6: Threat Management
This module explains Microsoft Threat Management which provides you with the tools to evaluate and address cyber threats and formulate responses. You will learn how to use the Security dashboard and Azure Sentinel for Microsoft 365.

Lessons

- Security dashboard
- Threat investigation and response
- Azure Sentinel
- Advanced Threat Analytics

Lab: Using Attack Simulator

- Conduct a simulated Spear phishing attack
- Conduct simulated password attacks

After completing this module, delegates will be able to:

- Describe how Threat Explorer can be used to investigate threats and help to protect your tenant.
- Describe how the Security Dashboard gives C-level executives insight into top risks and trends.
- Describe what Advanced Thread Analytics (ATA) is and what requirements are needed to deploy it.
- Configure Advanced Threat Analytics.
- Use the attack simulator in Microsoft 365.
- Describe how Azure Sentinel can used for Microsoft 365.

Module 7: Microsoft Cloud Application Security
This module focuses on cloud application security in Microsoft 365. The module will explain cloud discovery, app connectors, policies, and alerts. You will learn how these features work to secure you cloud applications.

Lessons

- Deploy Cloud Application Security
- Use cloud application security information

After completing this module, delegates will be able to:

- Describe Cloud App Security.
- Explain how to deploy Cloud App Security.
- Control your Cloud Apps with Policies.
- Use the Cloud App Catalog.
- Use the Cloud Discovery dashboard.
- Manage cloud app permissions.

Module 8: Mobility
This module focuses on securing mobile devices and applications. You will learn about Mobile Device Management and how it works with Microsoft Intune. You will also learn about how Intune and Azure AD can be used to secure mobile applications.

Lessons

- Mobile Application Management (MAM)
- Mobile Device Management (MDM)
- Deploy mobile device services
- Enroll devices to Mobile Device Management

Lab: Device Management

- Enable Device Management
- Configure Azure AD for Intune
- Create compliance and conditional access policies

After completing this module, delegates will be able to:

- Describe mobile application considerations.
- Manage devices with MDM.
- Configure Domains for MDM.
- Manage Device Security Policies.
- Enrol devices to MDM.
- Configure a Device Enrolment Manager Role.

Module 9: Information Protection and Governance
This module focuses on data loss prevention in Microsoft 365. You will learn about how to create policies, edit rules, and customize user notifications to protect your data.

Lessons

- Information protection concepts
- Governance and Records Management
- Sensitivity labels
- Archiving in Microsoft 365
- Retention in Microsoft 365
- Retention policies in the Microsoft 365 Compliance Center
- Archiving and retention in Exchange
- In-place records management in SharePoint

Lab: Archiving and Retention

- Initialize compliance
- Configure retention tags and policies

After completing this module, delegates will be able to:

- Configure sensitivity labels.
- Configure archiving and retention in Microsoft 365.
- Plan and configure Records Management.

Module 10: Rights Management and Encryption
This module explains information rights management in Exchange and SharePoint. The module also describes encryption technologies used to secure messages.

Lessons

- Information Rights Management (IRM)
- Secure Multipurpose Internet Mail Extension (S-MIME)
- Office 365 Message Encryption

Lab: Configure Office 365 Message Encryption

- Configure Office 365 Message Encryption
- Validate Information Rights Management

After completing this module, delegates will be able to:

- Describe the various Microsoft 365 Encryption Options.
- Describe the use of S/MIME.
- Describe and enable Office 365 Message Encryption.

Module 11: Data Loss Prevention
This module focuses on data loss prevention in Microsoft 365. You will learn about how to create policies, edit rules, and customize user notifications to protect your data.

Lessons

- Data loss prevention fundamentals
- Create a DLP policy
- Customize a DLP policy
- Create a DLP policy to protect documents
- Policy tips

Lab: Implement Data Loss Prevention policies

- Manage DLP Policies
- Test MRM and DLP Policies

After completing this module, delegates will be able to:

- Describe Data Loss Prevention (DLP).
- Use policy templates to implement DLP policies for commonly used information.
- Configure the correct rules for protecting content.
- Describe how to modify existing rules of DLP policies.
- Configure the user override option to a DLP rule.
- Explain how SharePoint Online creates crawled properties from documents.

Module 12: Compliance Management

- This module explains the Compliance center in Microsoft 365. It discusses the components of compliance score.

Lessons

- Compliance center

After completing this module, delegates will be able to:

- Describe how to use compliance score to make organizational decisions.
- Describe how assessments are used to determine compliance score.

Module 13: Insider Risk Management
This module focuses on insider risk related functionality within Microsoft 365. It covers not only Insider Risk Management in the compliance center but also information barriers and privileged access management as well.

Lessons

- Insider Risk
- Privileged Access
- Information barriers
- Building ethical walls in Exchange Online

Lab: Privileged Access Management

- Set up privileged access management and process a request

After completing this module, delegates will be able to:

- Explain and configure Insider Risk Management in Microsoft 365.
- Configure and approve privileged access requests for global administrators.
- Configure and use information barriers to conform to organizational regulations.
- Build ethical walls in Exchange Online.
- Configure Customer Lockbox.

Module 14: Discover and Respond
This module focuses on content search and investigations. The module covers how to use eDiscovery to conduct advanced investigations of Microsoft 365 data. It also covers audit logs and discusses GDPR data subject requests.

Lessons

- Content Search
- Audit Log Investigations
- Advanced eDiscovery

Lab: Manage Search and Investigation

- Investigate your Microsoft 365 Data
- Conduct a Data Subject Request

After completing this module, delegates will be able to:

- Conduct content searches in Microsoft 365.
- Perform and audit log investigation.
- Configure Microsoft 365 for audit logging.
- Use Advanced eDiscovery.

Exam Details

This course leads to the MS-500 Microsoft 365 Security Administration exam, which will earn you the Microsoft 365 Certified: Security Administrator Associate certification.

Building Applications and Solutions with Microsoft 365 Core Services

Course Code	MS600
Duration	5 days

Overview

This course covers five central elements of Microsoft 365 platform – implementing Microsoft Identity, working with Microsoft Graph, extending and customizing SharePoint, extending Teams, and extending Office. In this course, delegates will learn how to implement Microsoft Identity and work with Microsoft Graph. Delegates will also gain the knowledge on UI elements (including Adaptive Cards and UI Fabric), Integration Points (including Microsoft Teams, Office Add-ins, SharePoint Framework, Actionable Messages), and determining workload platform targets. In implementing Microsoft Identity, delegates will learn to implement Microsoft identity including registering an application, implanting authentication, configuring permissions to consume an API, and creating a service to access Microsoft Graph. In working with Microsoft Graph, delegates will learn how to access user data, explore query parameters, manage a group lifecycle, access files, and optimize network traffic using Microsoft Graph. In extending and customizing SharePoint, delegates will learn about SharePoint Framework web parts, extensions, and how to package and deploy a SPFx solution. In extending Teams, delegates will look at the components of a Teams App, work with webhooks, tabs, and conversational bots. In extending Office, delegates work with Office Add-ins, task pane add-ins, JavaScript APIs, Office UI Fabric, and actionable messages with adaptive cards.

Audience

Delegates in this course are interested in Microsoft 365 development platform or in passing the Microsoft 365 Developer Associate certification exam. Delegates should also have 1-2 years' experience as a developer. This course assumes delegates know how to code and have a basic understanding of REST APIs, JSON, OAuth2, OData, OpenID Connect, Microsoft identities including Azure AD and Microsoft accounts, Azure AD B2C, and permission/consent concepts.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Implementing Microsoft Identity
- Working with Microsoft Graph
- Determining workload platform targets
- Integration Points, including Microsoft Teams, Office Add-ins, and SharePoint Framework

Prerequisites

- Delegates should have 1-2 years' experience as a developer. This course assumes delegates know how to code and have a basic understanding of REST APIs, JSON, OAuth2, OData, OpenID Connect, Microsoft identities including Azure AD and Microsoft accounts, Azure AD B2C, and permission/consent concepts.
- It is recommended that delegates have some experience developing solutions on Microsoft Teams, Office Add-ins, or SharePoint Framework through all phases of software development.

Course Contents

Module 1: Implement Microsoft Identity
In this module, you will learn to implement Microsoft identity including registering an application, implanting authentication, configuring permissions to consume an API, and creating a service to access Microsoft Graph.

Lessons

- Microsoft Identity platform
- Register an Application
- Implement Authentication
- Configure Permissions to consume an API
- Implement Authorization to consume an API
- Implement Authorization in an API
- Create a Service to access Microsoft Graph

Lab: Implement Microsoft Identity

- Registering an application in azure active directory
- Implementing Authentication
- Configuring permission to consume an API
- Implementing authorization to consume an API
- Implementing authorization in an API
- Creating a service to access Microsoft Graph

After completing this module, delegates will be able to:

- Register an application in Azure AD.
- Implement authentication.
- Configure permissions to consume an API.
- Create a service to access Microsoft Graph.

Module 2: Work with Microsoft Graph

In this module you will learn how to access user data, explore query parameters, manage a group lifecycle, access files, and optimize network traffic using Microsoft Graph.

Lessons

- What is Microsoft Graph
- Access user data from Microsoft Graph
- Data usage with query parameters
- Manage a group lifecycle on Microsoft Graph
- Access files with Microsoft Graph
- Optimize network traffic

Lab: Work with Microsoft Graph

- Querying User Data from the Microsoft Graph
- Using Query Parameters when querying Microsoft Graph via HTTP
- Retrieving and controlling information returned from Microsoft Graph
- Creating an Office 365 Group and Team
- Uploading files to OneDrive and SharePoint
- Using Change Notifications and Track Changes with Microsoft Graph
- Reducing traffic with batched requests
- Understanding throttling in Microsoft Graph

After completing this module, delegates will be able to:

- Access user data with Microsoft Graph.
- Work with data using queries on Microsoft Graph.
- Manage a group lifecycle on Microsoft Graph.
- Optimize network traffic using Microsoft Graph.

Module 3: Extend and Customize SharePoint

In this module you will learn about SharePoint Framework web parts, extensions, and how to package and deploy a SPFx solution.

Lessons

- SharePoint Framework web parts
- SharePoint Framework extensions
- Package and deploy a SPFx solution
- Consumption of Microsoft Graph
- Consumption of 3rd party APIs secured with Azure AD from within SPFx
- Web Parts as Teams Tabs
- Branding and theming in SharePoint

Lab: Extend and Customize SharePoint

- Introduction to SharePoint Framework (SPFx)
- Working with the web part property pane
- Creating SharePoint Framework Extensions
- Creating a Command Set Extension
- Creating a Field Customizer Extension
- Deploying a SharePoint Framework Solution
- Calling Azure AD Protected 3rd Party REST APIs
- Deploying SPFx Solutions to Microsoft Teams

After completing this module, delegates will be able to:

- Package and deploy a SharePoint Framework solution.
- Utilize consumption of Microsoft Graph.
- Work with web parts as Team Tabs.

Module 4: Extend Teams
In this module you will look at the components of a Teams App, work with webhooks, tabs, and conversational bots.

Lessons

- Microsoft Teams App
- Webhooks in Microsoft Teams
- Tabs in Microsoft Teams
- Messaging extensions in Microsoft Teams
- Conversational bots in Microsoft Teams

Lab: Extend Teams

- Understanding the components of a Teams App
- Working with webhooks in Microsoft Teams
- Creating tabs in Microsoft Teams
- Understanding messaging extensions
- Understanding conversational bots

After completing this module, delegates will be able to:

- Recognize the components of a Teams App.
- Work with webhooks in Microsoft Teams.
- Create tabs in Microsoft Teams.
- Create and register outgoing webhooks.

Module 5: Extend Office
In this module you will work with Office Add-ins, task pane add-ins, JavaScript APIs, Office UI Fabric, and actionable messages with adaptive cards.

Lessons

- Office Add-ins
- Office JS APIs
- Customization of Add-ins
- Testing, debugging, and deployment options
- Actionable message

Lab: Extend Office

- Understanding fundamental components and types of Office Add-ins
- Understanding Office JavaScript APIs
- Understanding customization of Add-ins
- Understanding actionable messages

After completing this module, delegates will be able to:

- Understanding fundamental components and types of Office Add-ins.
- Understanding Office JavaScript APIs.
- Understanding customization of Add-ins.
- Understanding actionable messages.

Exam Details

This course leads to the MS-600 Building Applications and Solutions with Microsoft 365 Core Services exam, which will earn you the Microsoft 365 Certified: Developer Associate certification.

Managing Microsoft Teams

Course Code	MS700
Duration	4 days

Overview

The Managing Microsoft Teams course is designed for persons who are aspiring to the Microsoft 365 Teams Admin role. Microsoft Teams admins configure, deploy, and manage Office 365 workloads for Microsoft Teams that focus on efficient and effective collaboration and communication in an enterprise environment. This course covers six central elements - Microsoft Teams overview, implementing governance, security and compliance for Microsoft Teams, preparing the environment for a Microsoft Teams deployment, deploying and managing teams, managing collaboration and managing communication in Microsoft Teams. In Microsoft Teams overview, you will get an overview of Microsoft Teams including Teams architecture and related Office 365 workloads. You will be provided an overview of security and compliance in Microsoft Teams and finally get an overview of how to manage Microsoft Teams. In implementing governance, security and compliance for Microsoft Teams, you will plan and configure governance for Office 365 groups including expiration and naming policies. Then you will implement security by configuring conditional access, MFA or Threat Management for Microsoft Teams. Finally, you will implement compliance for Teams by using DLP policies, eDiscovery cases or supervision policies. In preparing the environment for a Microsoft Teams deployment, you plan an upgrade from Skype for Business to Microsoft Teams by evaluating upgrade paths with coexistence and upgrade modes, manage meeting migrations and configuring coexistence and upgrade settings. Then you plan and configure network settings for Microsoft Teams, and finally you will deploy and manage Microsoft Teams endpoints. In deploying and managing teams, you will learn how to create and manage teams, manage membership and access for both, internal and external users. In managing collaboration in Microsoft Teams, you will manage chat and collaboration experiences such as team settings or private channel creation policies. Finally, you will manage settings for Teams apps such as app setup policies, Apps, bots & connectors in Microsoft Teams or publish a custom app in Microsoft Teams. This course concludes with managing communication in Microsoft Teams. You will learn how to manage Live event and meetings experiences, manage phone numbers or Phone System for Microsoft Teams and finally how to troubleshoot audio, video, and client issues.

Audience

Delegates in this course are interested in Microsoft Teams or in passing the Microsoft Teams Administrator Associate certification exam.

Learning Objectives

By actively participating in this course, you will learn about the following:

- What is Microsoft Teams and how the components work together.
- How to implement Governance, Security and Compliance for Microsoft Teams.
- How to prepare an organizations environment for a Microsoft Teams deployment.
- How to deploy and manage teams.
- Ways of managing collaboration in Microsoft Teams.
- Techniques to manage and troubleshoot communication in Microsoft Teams.

Prerequisites

- A proficient understanding of basic functional experience with Microsoft 365 services.
- A proficient understanding of general IT practices, including using PowerShell.

Course Contents

Module 1: Microsoft Teams Overview
In Microsoft Teams overview, you will get an overview of Microsoft Teams including Teams architecture and related Office 365 workloads. You will be provided an overview of security and compliance in Microsoft Teams and finally get an overview of how to manage Microsoft Teams.

Lessons

- Overview of Microsoft Teams
- Overview of security and compliance in Microsoft Teams
- Overview of managing Microsoft Teams

Lab: Manage roles and create teams

- Prepare team roles and licenses
- Create new team

Module 2: Implement Microsoft Teams Governance, Security and Compliance
In implementing governance, security and compliance for Microsoft Teams, you will plan and configure governance for Office 365 groups including expiration and naming policies. Then you will implement security by configuring conditional access, MFA or Threat Management for Microsoft Teams. Finally, you will implement compliance for Teams by using DLP policies, eDiscovery cases or supervision policies.

Lessons

- Implement Governance and Lifecycle Management for Microsoft Teams
- Implementing Security for Microsoft Teams
- Implementing Compliance for Microsoft Teams

Lab: Configure Security and Compliance for teams and content

- Implement Governance and Lifecycle Management for Microsoft Teams
- Implementing security for Microsoft Teams
- Implementing compliance for Microsoft Teams

Module 3: Prepare the environment for a Microsoft Teams deployment
In preparing the environment for a Microsoft Teams deployment, you plan an upgrade from Skype for Business to Microsoft Teams by evaluating upgrade paths with coexistence and upgrade modes, manage meeting migrations and configuring coexistence and upgrade settings. Then you plan and configure network settings for Microsoft Teams, and finally you will deploy and manage Microsoft Teams endpoints.

Lessons

- Upgrade from Skype for Business to Microsoft Teams
- Plan and configure network settings for Microsoft Teams
- Deploy and Manage Microsoft Teams endpoints

Lab: Environment preparation for Teams

- Calculate networking capabilities
- Evaluate configuration profiles
- Provide team resources

Module 4: Deploy and manage teams
In deploying and managing teams, you will learn how to create and manage teams, manage membership and access for both, internal and external users.

Lessons

- Create and manage teams
- Manage membership
- Manage access for external users

Lab: Manage teams

- Manage team resources
- Manage sharing and access

Module 5: Manage collaboration in Microsoft Teams
In managing collaboration in Microsoft Teams, you will manage chat and collaboration experiences such as team settings or private channel creation policies. Finally, you will manage settings for Teams apps such as app setup policies, Apps, bots & connectors in Microsoft Teams or publish a custom app in Microsoft Teams.

Lessons

- Manage chat and collaboration experiences
- Manage settings for Teams apps

Lab: Modify collaboration settings for Teams

- Configure channel and message policies
- Manage app settings for team

Module 6: Manage communication in Microsoft Teams
This course concludes with managing communication in Microsoft Teams. You will learn how to manage Live event and meetings experiences, manage phone numbers or Phone System for Microsoft Teams and finally how to troubleshoot audio, video, and client issues.

Lessons

- Manage Live event and meetings experiences
- Manage phone numbers
- Manage Phone System for Microsoft Teams
- Troubleshot audio, video, and client issues

Lab: Modify communication settings for Teams

- Configure meeting policies
- Manage Phone System for Microsoft Teams
- Troubleshooting audio, video and client issues

Exam Details

This course leads to the MS-700 Managing Microsoft Teams exam, which will earn you the Microsoft 365 Certified: Teams Administrator Associate certification.

skilltec training

Moving forward in knowledge and training

Microsoft Teams Voice Engineer

Course Code	MS720
Duration	3 days

Overview

In this course, you will learn how to plan, design, configure, maintain, and troubleshoot an integrated communications solution at an organization using Microsoft Teams. The course will cover Teams Phone with Calling Plans, Direct Routing, and Operator Connect, in addition to Teams devices, audio/video conferencing, and voice migration. Students will learn troubleshooting methodologies and how to resolve common telephony and voice problems.

Audience

The Microsoft Teams Voice Engineer plans, designs, configures, maintains, and troubleshoots an integrated communications solution at an organization. The Microsoft Teams Voice Engineer must be able to translate business requirements into technical architecture and designs for communication solutions. The Microsoft Teams Voice Engineer is familiar with telecommunication technologies and has experience in Microsoft Teams, Microsoft 365, and PowerShell. They must be able to deploy and configure Microsoft Teams Phone with PSTN connectivity through Direct Routing, Operator Connect, and Teams Calling Plans. The Microsoft Teams Voice Engineer manages Teams-certified devices, audio/video conferencing, and voice migration. The Microsoft Teams Voice Engineer collaborates with telephony providers and third-party vendors to enable advanced voice features in Microsoft Teams. The Microsoft Teams Voice Engineer also works with administrators for other workloads, including networking, identity, licensing, security, and compliance.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Plan and Configure Microsoft Teams Phone
- Plan and optimize network performance for Teams Phone
- Configure and deploy Direct Routing
- Configure, deploy, and manage Teams devices
- Monitor and Troubleshoot Teams Phone

Prerequisites

To earn the Microsoft Teams Voice Engineer certification, candidates must pass Exam MS-700: Managing Microsoft Teams in addition to the MS-720 exam

Course Contents

Module 1: Plan and configure Teams Phone
After completing module 1, students will learn how to plan for and configure Teams Phone, including Calling Plans, Direct Routing, Auto Attendants, Call Queues, Operator Connect, and how to extend Teams Phone with additional services.

Lessons M1

- Plan Teams Phone
- Plan and optimize network performance for Teams Phone
- Migrate Voice Services from Skype for Business Server to Teams
- Configure Teams Phone
- Configure Auto Attendants and Call Queues
- Configure and deploy Direct Routing
- Extend Teams Phone with additional services

Lab: Prepare the lab environment

- Configure your lab environment
- Assign permissions

Lab: Plan for Teams Voice

- Validate licenses and devices

Lab: Configure your environment for Teams Voice Usage

- Evaluate your network with the Network Planner
- Use the Network Testing Tool
- Configure a basic network topology
- Configure Voice Policies
- Configure Emergency Calling
- Configure Audio Conferencing Settings
- Prepare users for calling
- Configure call queues and auto attendants

Lab: Expand your Teams Voice Environment to use Direct Routing

- Configure the session border controller
- Configure direct routing settings
- Test direct routing configuration

After completing this module, students will be able to:

- Plan and Configure Microsoft Teams Phone
- Plan and optimize network performance for Teams Phone
- Configure and deploy Direct Routing

Lab: Manage your Teams Voice Environment

- Manage voice users
- Manage Teams devices
- Monitor and Troubleshoot Teams Phone

After completing this module, students will be able to:

- Manage voice users
- Configure, deploy, and manage Teams devices
- Monitor and Troubleshoot Teams Phone

Module 2: Manage Teams Phone

In this module, students will learn how to configure Teams Phone users, devices, and troubleshoot Teams Phone voice issues.

Lessons M2

Configure and manage voice users

- Configure, deploy and manage Teams devices
- Monitor and Troubleshoot Teams Phone

Lab: Migrate Voice Services from Skype for Business to Teams

- Configure hybrid environment
- Migrate users to Teams

Lab: Manage your Teams Voice Environment

- Manage voice users
- Manage Teams devices
- Monitor and Troubleshoot Teams Phone

After completing this module, students will be able to:

- Manage voice users
- Configure, deploy, and manage Teams devices
- Monitor and Troubleshoot Teams Phone

Exam Details

This course leads to the MS-720 Teams Voice Engineer exam, which will earn you the Microsoft 365 Certified: Teams Voice Engineer certification.

Microsoft 365 Fundamentals

Course Code	MS900
Duration	2 days

Overview

This course provides foundational knowledge on the considerations and benefits of adopting cloud services and the Software as a Service (SaaS) cloud model, with a specific focus on Microsoft 365 cloud service offerings. You will begin by learning about cloud fundamentals, including an overview of cloud computing and specifically Microsoft cloud services. You will be introduced to Microsoft Azure, and you will examine the differences between Microsoft 365 and Office 365. You will then perform an in-depth review of Microsoft 365, including a comparison of Microsoft on-premises services versus Microsoft 365 cloud services, a review of enterprise mobility in Microsoft 365, and an analysis of how Microsoft 365 services provide collaboration. The course then analyzes how security, compliance, privacy, and trust are handled in Microsoft 365, and it concludes with a review of Microsoft 365 subscriptions, licenses, billing, and support.

Audience

This course is designed for Business Decision Makers and IT Professionals who aspire to deploy cloud services in their organization, or who are simply looking to acquire foundational knowledge on cloud fundamentals. This includes the considerations and benefits of adopting cloud services in general and the Software as a Service (SaaS) cloud model specifically, with a general focus on Microsoft 365 cloud service offerings.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Differentiate between the various cloud service models.
- Identify the key differences between Microsoft 365 subscriptions.
- Plan for migration to Microsoft 365 services.
- Identify key differences between Microsoft on-premises services and Microsoft 365 cloud services.
- Identify how Microsoft 365 services support teamwork.
- Describe identities, including cloud, on-premises, and hybrid identity.
- Describe cloud device management and protection, including the use of Intune.
- Describe data protection, including the use of Azure Information Protection.
- Describe compliance in general and the compliance features in Microsoft 365.
- Describe Microsoft 365 subscriptions, licenses, billing, and support.

Prerequisites

- General knowledge of networking, computing, and cloud concepts

Course Contents

Module 1: Cloud concepts
Explore the core concepts of cloud computing and how it can help your business.
Lessons

- Principles of cloud computing
- What is Microsoft 365?
- Select a cloud deployment

Module 2: Microsoft 365 productivity and teamwork capabilities
Learn about the productivity and teamwork solutions in Microsoft 365 and the capabilities that help people be more productive using Microsoft 365 - The World's Productivity Cloud.
Lessons

- Microsoft 365 productivity and teamwork solutions
- Engage employees with Microsoft Stream, Teams, and Yammer
- Get more done with Office across all devices
- File storage and sharing with OneDrive and SharePoint

Module 3: Microsoft 365 business management capabilities
Learn about the business management solutions in Microsoft 365 and the capabilities that help organizations be more productive using Microsoft 365 - The World's Productivity Cloud.
Lessons

- Manage your business with Microsoft 365
- Simplify device management with Microsoft Endpoint Manager
- Get more done and stay secure with Windows 10
- Harness business intelligence with Microsoft 365 analytics and reporting

Module 4: Microsoft 365 security and compliance
Learn about the Microsoft 365 security and compliance solutions areas and the capabilities available to help enterprises secure their enterprise and meet regulatory requirements.
Lessons

- Security principles and solution areas
- Identity and access management
- Threat protection
- Cloud security
- Information protection and governance
- Compliance management
- Manage risk, discovery, and audit

Module 5: Microsoft 365 Licensing and support
Learn more about Microsoft 365 licensing, service, and support options.
Lessons

- Identify licensing options available in Microsoft 365
- Describe support offerings in Microsoft 365 services
- Describe the service life cycle in Microsoft 365

Exam Details

This course leads to the MS-900 Microsoft 365 Fundamentals exam, which will earn you the Microsoft 365 Certified Fundamentals certification.

skilltec training

Moving forward in knowledge and training

Microsoft Power Platform App Maker

Course Code	MSPL100
Duration	3 days

Overview

This course will teach you how to build apps with low-code techniques to simplify, automate, and transform business tasks and processes using Microsoft Power Platform'.

Audience

The App Maker builds solutions to simplify, automate, and transform tasks and processes for themselves and their team where they have deep expertise in the solution business domain. They have basic data modelling, user experience design, requirements analysis, and process analysis skills. The App Maker creates and enforces business processes, structures digital collection of information, improves efficiency of repeatable tasks, and automates business processes.

The App Maker uses the Maker tools of Power Platform to solve business problems. They may use advanced features of Microsoft apps and third-party productivity tools. The App Maker is aware of the capabilities and limitations of available tools and understands how to apply them. The App Maker is self-directed, and solution focused. They may not have formal IT training but are comfortable using technology to solve business problems with a personal growth mindset. They understand the operational need and have a vision of the desired outcome. They approach problems with phased and iterative strategies.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Design apps and automate workflows
- Create apps and automate workflows
- Analyze and visualize data in context of an app or automated workflow
- Implement and manage apps and automated workflows

Prerequisites

- Basic data modelling, user experience design, requirements analysis, and process analysis skills.
- A personal growth mindset and are comfortable using technology to solve business problems.
- An understanding of the operational need and have a vision of the desired outcome. They approach problems with phased and iterative strategies.

Course Contents

Module 1: Create a model-driven application in Power Apps
This module introduces you to creating a model-driven app in Power Apps that uses Common Data Service.

Module 2: Create a canvas app in Power Apps
This module introduces you to Power Apps, helps you create and customize an app, and then manage and distribute it

Module 3: Use the UI and controls in a canvas app in Power Apps
This module will focus on how to provide the best app navigation, and build the best UI using themes, icons, images, personalization, different form factors, and controls.

Module 4: Automate a business process using Power Automate
This module introduces you to Power Automate, teaches you how to build workflows, and how to administer flows

Module 5: Create and use analytics reports with Power BI
Learn what Power BI is, including its building blocks and how they work together

Module 6: Get started with AI Builder
This module helps you build an AI model from the beginning and shows how you can use it in your business without writing a single line of code

Exam Details

This course helps you to prepare for the Microsoft exam M-PL100.

Please note that whilst this course is aligned to the equivalent Microsoft Exam it may not contain all information required to pass the exam. As per Microsoft guidance, further self-study and hands on experience is recommended in addition to attendance of this course.

Microsoft Power Platform Functional Consultant

Course Code	MPL200
Duration	4 days

Overview

The Power Platform empowers organizations to automate business processes, develop their own rich app experiences, and connect with customers better and faster. In this course, students will learn to perform discovery, capture requirements, engage subject matter experts and stakeholders, translate requirements, and configure Power Platform solutions and apps. They will supplement their learnings with hands-on labs to create application enhancements, custom user experiences, system integrations, data conversions, custom process automation, and custom visualizations. Power Platform is comprised of four key products: Power Apps, Power Automate, Power BI, and Power Virtual Agents. In this course, we will cover these four applications in depth, with additional focus on the Common Data Service, AI Builder, connectors, and portals.

Audience

A Power Platform Functional Consultant is responsible for performing discovery, capturing requirements, engaging subject matter experts and stakeholders, translating requirements, and configuring Power Platform solutions and apps. The Functional Consultant implements components of a solution that include application enhancements, custom user experiences, system integrations, data conversions, custom process automation, and custom visualizations.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Work with an organization to gather requirements and implement Power Platform solutions
- Build model-driven, canvas, and portal apps
- Create Power Automate flows
- Design a simple chatbot using Power Virtual Agents
- Analyze data using Power BI visualizations and dashboards

Prerequisites

- Experience as an IT professional or student
- Working knowledge of the Power Platform and its key components
- A knowledge of the Common Data Service and security concepts

Course Contents

Module 1: Introduction to the Power Platform
This module will provide the learner with background about the Power Platform and its 4 key components: Power Apps, Power Automate, Power BI, and Power Virtual Agents.

Lessons of Module 1

- Power Platform overview

Lab 1: Validate lab environment

After completing module 1, students will be able to:

- Identify the key components of the Power Platform
- Describe the role of a functional consultant

Module 2: Work with the Common Data Service
In this module, students will learn about creating a data model in the Common Data Service, including importing data, using tabular reporting options, and configuring security. They will also learn about creating easy AI with AI Builder.

Lessons of Module 2

- Work with the data model
- Create and manage processes
- Work with AI Builder
- Configure Common Data Service settings
- Import and export data
- Use tabular reporting options
- Configure security settings

Lab 2a: Create an app
Lab 2b: Create entities and fields
Lab 2c: Create relationships
Lab 2d: Additional entity options

After completing module 2, students will be able to:

- Create a data model
- Configure Common Data Service settings
- Configure security

Module 3: Make Power Apps
In this module, students will learn the business value of the three types of Power Apps. They will then learn to how to configure and design them, including user experience considerations for each type of application.

Lessons of Module 3

- Make model-driven apps
- Make canvas apps
- Make portal apps

Lab 3a: App designer
Lab 3b: Modify forms
Lab 3c: Modify views
Lab 3d: Build dashboards
Lab 3e: Canvas app fundamentals
Lab 3f: Work with data and services
Lab 3g: User experience

After completing module 3, students will be able to:

- Create and design a Power App
- Connect a Power App to data
- Design app navigation

Module 4: Build Power Automate flows
In this module, students will learn how to automate business processes using Power Automate flows, business process flows, and UI flows.

Lessons of Module 4

- Build flows
- Build business process flows
- Build UI flows

Lab 4a: Create users
Lab 4b: Create security role
Lab 4c: Configure a new business rule
Lab 4d: Advanced business rules
Lab 4e: Create a flow
Lab 4f: Build approval flow
Lab 4g: Build a business process flow
Lab 4h: Add branching to business process flow

After completing module 4, students will be able to:

- Automate business processes using flows
- Connect to data in Power Automate
- Create a business process flow with branching logic

Module 5: Work with Power Virtual Agents
In this module, students will learn how to automate customer interactions with a chatbot using Power Virtual Agents.

Lessons of module 5

- Create a chatbot
- Configure topics
- Automate and integrate
- Configure entities
- Test and publish chatbots

Lab 5: Create a chatbot

After completing module 5, students will be able to:

- Configure topics, entities, and variables
- Create a chatbot
- Integrate with Omnichannel for Customer Service
- Work in the PVA interface

Module 6: Analyze data with Power BI
In this module, students will learn how to work with Power BI Desktop and Power BI Service to analyze data and create visualizations.

Lessons of Module 6

- Get started with Power BI
- Model data in Power BI
- Create visualizations
- Create dashboards
- Publish and share in Power BI

Lab 6a: Build a Word template
Lab 6b: Build an Excel template
Lab 6c: Duplicate detection
Lab 6d: Import data
Lab 6e: Export data
Lab 6f: Bulk delete

After completing module 6, students will be able to:

- Create visualizations
- Consume data in Power BI
- Export data visualizations for stakeholders

Module 7: Consultant skills
In this module, students will learn more about the functional consultant role and the skills required to successfully implement a Power Platform solution for an organization.

Lessons of module 7

- Consultant skills overview
- Create and validate documentation
- Engage stakeholders
- Perform quality assurance
- Configure integrations

After completing module 7, students will be able to:

- Identify appropriate documentation
- Write a business requirement
- Engage stakeholders with demos
- Participate in ALM and testing

Exam Details

This course helps you to prepare for the M-PL200 Exam.

Please note that whilst this course is aligned to the equivalent Microsoft Exam it may not contain all information required to pass the exam. As per Microsoft guidance, further self-study and hands on experience is recommended in addition to attendance of this course.

Microsoft Power BI Data Analyst

Course Code	MPL300
Duration	3 days

Overview

This course will discuss the various methods and best practices that are in line with business and technical requirements for modeling, visualizing, and analyzing data with Power BI. The course will also show how to access and process data from a range of data sources including both relational and non-relational data. This course will also explore how to implement proper security standards and policies across the Power BI spectrum including datasets and groups. The course will also discuss how to manage and deploy reports and dashboards for sharing and content distribution. Finally, this course will show how to build paginated reports within the Power BI service and publish them to a workspace for inclusion within Power BI.

Audience

The audience for this course are data professionals and business intelligence professionals who want to learn how to accurately perform data analysis using Power BI. This course is also targeted toward those individuals who develop reports that visualize data from the data platform technologies that exist on both in the cloud and on-premises.

Learning Objectives

By actively participating in this course, you will learn about the following:

- 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

Prerequisites

- Understanding core data concepts.
- Knowledge of working with relational data in the cloud.
- Knowledge of working with non-relational data in the cloud.
- Knowledge of data analysis and visualization concepts. You can gain the prerequisites and a better understanding of working with data in Azure.

Course Contents

Module 1: Get Started with Microsoft Data Analytics

This module explores the different roles in the data space, outlines the important roles and responsibilities of a Data Analysts, and then explores the landscape of the Power BI portfolio.

- Data Analytics and Microsoft
- Getting Started with Power BI

Lab : Getting Started in Power BI Desktop

- Getting Started

After completing this module, students will be able to:

- Explore the different roles in data
- Identify the tasks that are performed by a data analyst
- Describe the Power BI landscape of products and services
- Use the Power BI service

Module 2: Prepare Data in Power BI

This module explores identifying and retrieving data from various data sources. You will also learn the options for connectivity and data storage and understand the difference and performance implications of connecting directly to data vs. importing it.

- Get data from various data sources

Lab : Preparing Data in Power BI Desktop

- Prepare Data

After completing this module, students will be able to:

- Identify and retrieve data from different data sources
- Understand the connection methods and their performance implications
- Use Microsoft Dataverse
- Connect to a data flow

Module 3: Clean, Transform, and Load Data in Power BI

This module teaches you the process of profiling and understanding the condition of the data. They will learn how to identify anomalies, look at the size and shape of their data, and perform the proper data cleaning and transforming steps to prepare the data for loading into the model.

- Data shaping
- Enhance the data structure
- Data Profiling

Lab : Transforming and Loading Data in Power BI Desktop

- Loading Data

After completing this module, students will be able to:

- Apply data shape transformations
- Enhance the structure of the data
- Profile and examine the data

Module 4: Design a Data Model in Power BI

This module teaches the fundamental concepts of designing and developing a data model for proper performance and scalability. This module will also help you understand and tackle many of the common data modeling issues, including relationships, security, and performance.

- Introduction to data modeling
- Working with tables
- Dimensions and Hierarchies

Lab : Data Modeling in Power BI Desktop

- Create Model Relationships
- Configure Tables
- Review the model interface
- Create Quick Measures

Lab : Advanced Data Modeling in Power BI Desktop

- Configure many-to-many relationships
- Enforce row-level security

After completing this module, students will be able to:

- Understand the basics of data modeling
- Define relationships and their cardinality
- Implement Dimensions and Hierarchies
- Create histograms and rankings

Module 5: Create Model Calculations using DAX in Power BI

This module introduces you to the world of DAX and its true power for enhancing a model. You will learn about aggregations and the concepts of Measures, calculated columns and tables, and Time Intelligence functions to solve calculation and data analysis problems.

- Introduction to DAX
- DAX context
- Advanced DAX

Lab : Advanced DAX in Power BI Desktop

- Use the CALCULATE() function to manipulate filter context
- Use Time Intelligence functions

Lab : Introduction to DAX in Power BI Desktop

- Create calculated tables
- Create calculated columns
- Create measures

After completing this module, students will be able to:

- Understand DAX
- Use DAX for simple formulas and expressions
- Create calculated tables and measures
- Build simple measures
- Work with Time Intelligence and Key Performance Indicators

Module 6: Optimize Model Performance in Power BI

In this module you are introduced to steps, processes, concepts, and data modeling best practices necessary to optimize a data model for enterprise-level performance.

- Optimze the model for performance
- Optimize DirectQuery Models
- Create and manage Aggregations

After completing this module, students will be able to:

- Understand the importance of variables
- Enhance the data model
- Optimize the storage model
- Implement aggregations

Module 7: Create Reports in Power BI

This module introduces you to the fundamental concepts and principles of designing and building a report, including selecting the correct visuals, designing a page layout, and applying basic but critical functionality. The important topic of designing for accessibility is also covered.

- Design a report
- Enhance the report

Lab : Designing a report in Power BI Desktop

- Create a live connection in Power BI Desktop
- Design a report
- Configure visual fields and format properties

Lab : Enhancing reports with interaction and formatting in Power BI Desktop

- Create and configure Sync Slicers
- Create a drillthrough page
- Apply conditional formatting
- Create and use Bookmarks

After completing this module, students will be able to:

- Design a report page layout
- Select and add effective visualizations
- Add basic report functionality
- Add report navigation and interactions
- Improve report performance
- Design for accessibility

Module 8: Create Dashboards in Power BI

In this module you will learn how to tell a compelling story through the use of dashboards and the different navigation tools available to provide navigation. You will be introduced to features and functionality and how to enhance dashboards for usability and insights.

- Create a Dashboard
- Real-time Dashboards
- Enhance a Dashboard

Lab : Creating a Dashboard in Power BI Service

- Create a Dashboard
- Pin visuals to a Dashboard
- Configure a Dashboard tile alert
- Use Q&A to create a dashboard tile

After completing this module, students will be able to:

- Create a Dashboard
- Understand real-time Dashboards
- Enhance Dashboard usability

Module 9: Enhance reports for usability and storytelling in Power BI

This module will teach you about paginated reports, including what they are how they fit into Power BI. You will then learn how to build and publish a report.

- Paginated report overview
- Create Paginated reports

Lab : Creating a Paginated report in Power BI Desktop

- Use Power BI Report Builder
- Design a multi-page report layout
- Define a data source
- Define a dataset
- Create a report parameter
- Export a report to PDF

After completing this module, students will be able to:

- Explain paginated reports
- Create a paginated report
- Create and configure a data source and dataset
- Work with charts and tables
- Publish a report

Module 10: Perform Advanced Analytics in Power BI

This module helps you apply additional features to enhance the report for analytical insights in the data, equipping you with the steps to use the report for actual data analysis. You will also perform advanced analytics using AI visuals on the report for even deeper and meaningful data insights.

- Advanced Analytics
- Data Insights through AI visuals

Lab : Data Analysis in Power BI Desktop

- Create animated scatter charts
- Use the visual to forecast values
- Work with Decomposition Tree visual
- Work with the Key Influencers visual

After completing this module, students will be able to:

- Explore statistical summary
- Use the Analyze feature
- Identify outliers in data
- Conduct time-series analysis
- Use the AI visuals
- Use the Advanced Analytics custom visual

Module 11: Manage Datasets in Power BI

In this module you will learn the concepts of managing Power BI assets, including datasets and workspaces. You will also publish datasets to the Power BI service, then refresh and secure them.

- Parameters
- Datasets
- Security in Power BI

After completing this module, students will be able to:

- Create and work with parameters
- Manage datasets
- Configure dataset refresh
- Troubleshoot gateway connectivity
- Understand the aspects of Power BI security
- Configure row-level security roles and group memberships

Module 12: Create and Manage Workspaces in Power BI
This module will introduce you to Workspaces, including how to create and manage them. You will also learn how to share content, including reports and dashboards, and then learn how to distribute an App.

- Creating Workspaces
- Sharing and Managing Assets

Lab : Publishing and Sharing Power BI Content

- Map security principals to dataset roles
- Share a dashboard
- Publish an App

After completing this module, students will be able to:

- Create and manage a workspace
- Understand workspace collaboration
- Monitor workspace usage and performance
- Distribute an App

Exam Details

This course will help to prepare for exam PL-300.

Microsoft Power Platform Developer

Course Code	MSPL400
Duration	5 days

Overview

The Microsoft Power Platform helps organizations optimize their operations by simplifying, automating and transforming business tasks and processes. In this course, students will learn how to build Power Apps, Automate Flows and extend the platform to complete business requirements and solve complex business problems.

Audience

Candidates for this course design, develop, secure, and troubleshoot Power Platform solutions. Candidates implement components of a solution that include application enhancements, custom user experience, system integrations, data conversions, custom process automation, and custom visualizations. Candidates will gain applied knowledge of Power Platform services, including in-depth understanding of capabilities, boundaries, and constraints.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Create a technical design
- Configure Common Data Service
- Create and configure Power Apps
- Configure business process automation
- Extend the user experience
- Extend the platform
- Develop Integrations

Prerequisites

- Candidates should have an introductory knowledge of Power Platform
- Candidates should have development experience that includes JavaScript, JSON, TypeScript, C#, HTML, .NET, Microsoft Azure, Microsoft 365, RESTful Web Services, ASP.NET, and Power BI

Course Contents

Module 1: Create a model-driven application in Power Apps

This module introduces you to creating a model-driven app in Power Apps that uses Common Data Service.

- Introduction to model-driven apps and Common Data Service
- Get started with model-driven apps in Power Apps
- Create and manage entities in Common Data Service
- Create and manage fields within an entity in Common Data Service
- Working with option sets in Common Data Service
- Create a relationship between entities in Common Data Service
- Define and create business rules in Common Data Service
- Create and define calculation or rollup fields in Common Data Service
- Get started with security roles in Common Data Service

Module 2: Create a canvas app in Power Apps

This module introduces you to Power Apps, helps you create and customize an app, and then manage and distribute it. It will also show you how to provide the best app navigation, and build the best UI using themes, icons, images, personalization, different form factors, and controls.

- Get started with Power Apps
- Customize a canvas app in Power Apps
- Manage apps in Power Apps
- Navigation in a canvas app in Power Apps
- How to build the UI in a canvas app in Power Apps
- Use and understand Controls in a canvas app in Power Apps
- Document and test your Power Apps application

Module 3: Master advance techniques and data options in canvas apps

This module will help you use advanced formulas, perform custom updates, performance checks and testing. It will also help you to improve user's experience, use custom connectors and focus on working with data source limits.

- Use imperative development techniques for canvas apps in Power Apps
- Author an advanced formula that uses tables, records, and collections in a canvas app in Power Apps
- Perform custom updates in a Power Apps canvas app
- Complete testing and performance checks in a Power Apps canvas app
- Work with relational data in a Power Apps canvas app
- Work with data source limits (delegation limits) in a Power Apps canvas app
- Connecting to other data in a Power Apps canvas app
- Use custom connectors in a Power Apps canvas app

Module 4: Automate a business process using Power Automate

This module introduces you to Power Automate, teaches you how to build workflows, and how to administer flows.

- Get started with Power Automate
- Build more complex flows with Power Automate
- Introduction to business process flows in Power Automate
- Create an immersive business process flow in Power Automate
- Understand advanced business process flow concepts in Power Automate
- Introduction to expressions in Power Automate

Module 5: Introduction to developing with Power Platform

This module is the first step in learning about platform, tools, and the ecosystem of the Power Platform

- Introduction to Power Platform developer resources
- Use developer tools to extend the Power Platform
- Introduction to extending the Microsoft Power Platform

Module 6: Extending the Power Platform Common Data Service
This module looks at the tools and resources needed for extending the Power Platform. We'll start with looking at the SDKs, the extensibility model, and event framework. This learning path also covers when to use plug-ins.

- Configuration of plug-ins as well as registering and deploying plug-ins.
- Introduction to Common Data Service for developers
- Extend plug-ins

Module 7: Extending the Power Platform user experience Model Driven apps
This module describes how to create client scripting, perform common actions with client script, and automate business process flow with client scrip. Learn about what client script can do, rules, and maintaining scripts.

- Discover when to use client script as well as when not to use client script.
- Introduction to web resources
- Performing common actions with client script
- Automate business process flows with client script

Module 8: Create components with Power Apps Component Framework
This module describes how to get started with Power Apps Component Framework with an introductory module on the core concepts and components. Then it shows you how to build a component and work with advanced Power Apps Component Framework features.

- Get started with Power Apps component framework
- Build a Power Apps component
- Use advanced features with Power Apps component framework

Module 9: Extend Power Apps portals
This module describes how to transform a content portal into a full web app interacting with Common Data Service. We will also cover the options available to customizers and developers to extend the portal functionality and integrate with Office 365, Power Platform, and Azure components.

- Introduction to Power Apps portals
- Access Common Data Service in Power Apps portals
- Extend Power Apps portals
- Build custom Power Apps portals web templates

Module 10: Integrate with Power Platform and Common Data Service
This module describes how to integrate with Common Data Service using code by learning about Common Data Service API. Get an in-depth overview of options available with Common Data Service to integrate data and events to Azure.

- Work with Common Data Service Web API
- Integrate Common Data Service Azure solutions

Exam Details

This course leads to the Microsoft exam MPL-400.

Please note that whilst this course is aligned to the equivalent Microsoft Exam it may not contain all information required to pass the exam. As per Microsoft guidance, further self-study and hands on experience is recommended in addition to attendance of this course.

Microsoft Power Platform Solution Architect

Course Code	MSPL600
Duration	4 days

Overview

The Solution Architect is responsible for the successful design, implementation, deployment and adoption of an overall solution. The Solution Architect ensures that the solution meets the customer's needs now and in the future. In this course, students will learn about decisions a Solution Architect makes during an implementation, covering security, integrations, Power Apps architecture, Power Automate architecture, and more. This course is designed to give you an introduction to the Solution Architect role.

Audience

Senior Consultants (both functional and technical) that aspire to be Solution Architects, or current Solution Architects that are new to the role.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Conceptualizing the design
- Project governance
- Power Platform architecture
- Data Modelling
- Analytics and artificial intelligence
- Lifecycle Management
- Power Automate Architecture
- Security Modelling
- Integration
- Dynamics 365 Applications architecture

Prerequisites

There are no Prerequisites for this course.

Course Contents

Module 1: Becoming a Solution Architect/Getting to know your customer
Lessons

- Define a Solution Architect
- Role of a Solution Architect on projects
- Project Methodology
- Getting to know your customer

Group exercise - Getting to know your customer

Module 2: Conceptualizing the design from requirements
Lessons

- How to lead the requirement collection effort
- Using fit gap analysis
- Pillars of good architecture
- Blueprinting the solution architecture

Group exercise - Design from requirements

Module 3: Project governance and working as a team
Lessons

- Solution Architect's role in project governance
- Techniques for keeping a project on track
- Scenarios that could cause a project to fail

Group exercise - Project governance and working as a team

Module 4: Power Platform Architecture
Lessons

- Key Power Platform architecture components
- Understand how platform design and limits influence solution architectures
- Updates and feature releases
- Understand how to communicate how the platform meets customer needs

Module 5: Data Modelling
Lessons

- Data model influences
- Data model strategy
- Data types
- Data relationships

Group exercise - Data modelling

Module 6: Analytics and artificial intelligence
Lessons

- Planning and evaluating requirements
- Operational reporting
- Power BI
- Enterprise BI
- Pre-built insights and custom AI

Module 7: Power Apps Architecture

Lessons

- Discuss options for apps and how to choose where to start
- Discuss app composition options
- Using components as part of your app architecture
- Considerations for including Portals as an app in your architecture

Group exercise - Power Apps Architecture topics

Module 8: Application Lifecycle Management (ALM)

Lessons

- Microsoft vision and Solution Architect's role in ALM
- Environment strategies
- Defining a solution structure for your deliverable

Lab: ALM Hands-on Lab

Module 9: Power Automate Architecture

Lessons

- Discuss options for automation and custom logic
- Review considerations for using triggers and common actions
- Explore using Business Process Flows (BPF) to guide users through business processes

Group Exercise - Evaluate scenarios for Power Automate usage

Module 10: Security Modelling

Lessons

- Solution Architect's role in security modelling
- Discovery and learning your client's environment
- Controlling access to environments and resources
- Controlling access to CDS Data

Group Exercise - Security Modelling

Module 11: Integration

Lessons

- Solution Architects role in Integrations
- What is an integration and why do we need it?
- Platform features that enable integration
- CDS Event Publishing
- Scenarios for group discussion

Module 12: Dynamics 365 Applications Architecture

Lessons

- Solution Architect's role when deploying Dynamics 365 apps
- Architecture Considerations for primary apps

Group Exercise - App specific working groups evaluate requirements

Module 13: Testing and Go Live

Lessons

- Solution Architect's role with testing and go live
- Planning for testing
- Planning for go live

Exam Details

This course helps you to prepare for the Microsoft exam M-PL600.

Please note that whilst this course is aligned to the equivalent Microsoft Exam it may not contain all information required to pass the exam. As per Microsoft guidance, further self-study and hands on experience is recommended in addition to attendance of this course.

skilltec training

Moving forward in knowledge and training

Microsoft Power Platform Fundamentals

Course Code	MSPL900
Duration	2 days

Overview

Learn the business value and product capabilities of Power Platform. Create a simple PowerApp, connect data with CDS, build a Power BI Dashboard, and automate a process with Microsoft Flow.

Audience

Candidates for this exam are users who aspire to improve productivity by automating business processes, analyzing data to produce business insights, and acting more effectively by creating simple app experiences.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describe the Power Platform components: Power Apps, Power BI and Microsoft Automate
- Describe the Power Platform components: Common Data Service, Connectors and AI builder
- Describe cross-cloud scenarios across M365, Dynamics 365, Microsoft Azure and 3rd party services
- Identify benefits and capabilities of Power Platform
- Identify the basic functionality and business value Power Platform components
- Implement simple solutions with Microsoft Automate, Power BI, and Power Apps

Prerequisites

There are no Prerequisites for this course.

Course Contents

Module 1: Introduction to Power Platform
Learn about the components of Power Platform, ways to connect data, and how organizations can leverage this technology to.

Lessons

- Power Platform Overview
- Module Summary

After completing this module, students will be able to:

- Identify when to use each Power Platform component application to create business solutions
- Learn the value of using Power Platform to create business solutions
- Learn the components and features of Power Platform

Module 2: Get Started with Power Apps
Learn about the value and capabilities of PowerApps, and ways other organizations have leveraged this technology to build simple applications for their business.

Lessons

- Power Apps Overview
- How to Build an App Solution
- Create Staff Canvas App
- Complete the App

Lab: How to Build a Basic Canvas App 2

- Create Security Canvas App

After completing this module, students will be able to:

- Learn how other organizations digitize their processes using Power Apps
- See Power Apps in action and learn options for making your first app
- Learn about what Power Apps is and its business value

Module 3: Introduction to Common Data Service
The Common Data Service allows you to delve into powerful, scalable data solutions in the cloud. Learn what makes the Common Data Service tick and how it can work with the Power Platform to create unique and efficient business solutions.

Lessons

- Common Data Service Overview
- Module Summary

Lab: Data Modelling

- Create Environment and Solution
- Create Entities and Relationships
- Import Data

After completing this module, students will be able to:

- Describe the difference between Common Data Service and Common Data Model
- Explain use cases and limitations of business rules and process flows
- Explain what environments, entities, fields, and relationships are in common data service

Module 4: Get Started with Power Automate
Learn how users can leverage Power Automate to improve business efficiency and productivity.

Lessons

- Power Automate Overview
- How to Build an Automated Solution

Lab: Build a Simple Flow

- Create Visit Notification Flow
- Create Security Sweep Flow

After completing this module, students will be able to:

- See how Power Automate works and looks from the user's perspective
- Build a simple flow
- Learn the business value and features of Power Automate

Module 5: Get Started with Power BI
Learn how organizations can use Power BI to easily clean, display, and understand data to ensure better informed decisions.

Lessons

- Power BI Overview
- How to Build a Simple Dashboard

Lab: Build a Power BI Report

After completing this module, students will be able to:

- See how Power BI works and looks from the user's perspective
- Learn how to build a simple Power BI dashboard
- Describe the business value and features of Power BI

Exam Details

This course helps you to prepare for the Microsoft exam M-PL900.

Please note that whilst this course is aligned to the equivalent Microsoft Exam it may not contain all information required to pass the exam. As per Microsoft guidance, further self-study and hands on experience is recommended in addition to attendance of this course.