Microsoft 365 Administrator: MS-102T00

Course Overview

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

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

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

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

Once you have this understanding of Microsoft 365's security suite, you then examine the key components of Microsoft 365 compliance management. This begins with an overview of all key aspects of data governance, including data archiving and retention, Microsoft Purview message encryption, and data loss prevention (DLP). You then delve deeper into archiving and retention, paying particular attention to Microsoft Purview insider risk management, information barriers, and DLP policies. You then examine how to implement these compliance features by using data classification and sensitivity labels.

Audience Profile

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

Prerequisites

Before attending this course, students must have:

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

Duration: 30 hrs (10 x 3hrs)

CONNECT **E-mail:** info@lgitsmart.co.za | **Web**: www.lgit.co.za

Course Outline

Module 1: Configure your Microsoft 365 experience

In this learning path, 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 Identity Protection and Microsoft Defender for Office 365.

Lessons

- Explore your Microsoft 365 cloud environment
- Configure your Microsoft 365 organizational profile
- Manage your tenant subscriptions in Microsoft 365
- Integrate Microsoft 365 with customer engagement apps
- Complete your tenant configuration in Microsoft 365

Module 2: Manage users, licenses, and mail contacts in Microsoft 365

This module provides instructions on how to create and manage user accounts, assign Microsoft 365 licenses to users, recover deleted user accounts, and create and manage mail contacts.

Lessons

- Determine the user identity model for your organization
- Create user accounts in Microsoft 365
- Manage user account settings in Microsoft 365
- Manage user licenses in Microsoft 365
- Recover deleted user accounts in Microsoft 365
- Perform bulk user maintenance in Azure Active Directory
- Create and manage guest users
- Create and manage mail contacts

Module 3: Manage groups in Microsoft 365

This module provides instructions on how to create groups for distributing email to multiple users within Exchange Online. It also explains how to create groups to support collaboration in SharePoint Online.

Lessons

- Plan a custom domain for your Microsoft 365 deployment
- Plan the DNS zones for a custom domain
- Plan the DNS record requirements for a custom domain
- Create a custom domain in Microsoft 365

Module 4: Add a custom domain in Microsoft 365

This module provides instruction on how to add a custom domain to your Microsoft 365 deployment. It also examines the DNS requirements that are necessary to support a new domain.

Lessons

- Examine groups in Microsoft 365
- Create and manage groups in Microsoft 365
- Create dynamic groups using Azure rule builder
- Create a Microsoft 365 group naming policy
- Create groups in Exchange Online and SharePoint Online

Module 5: Configure client connectivity to Microsoft 365

This module examines how clients connect to Microsoft 365. It also provides instructions on how to configure name resolution and Outlook clients, and how to troubleshoot client connectivity.

- Examine how automatic client configuration works
- Explore the DNS records required for client configuration
- Configure Outlook clients
- Troubleshoot client connectivity

Module 6: Configure administrative roles in Microsoft 365

This module examines the key functionality that's available in the more commonly used Microsoft 365 admin roles. It also provides instructions on how to configure these roles.

Lessons

- Explore the Microsoft 365 permission model
- Explore the Microsoft 365 admin roles
- Assign admin roles to users in Microsoft 365
- Delegate admin roles to partners
- Manage permissions using administrative units in Azure Active Directory
- Elevate privileges using Azure AD Privileged Identity Management
- Examine best practices when configuring administrative roles

Module 7: Manage tenant health and services in Microsoft 365

This module examines how to monitor your organization's transition to Microsoft 365 using Microsoft 365 tools. It also examines how to develop an incident response plan and request assistance from Microsoft.

Lessons

- Monitor the health of your Microsoft 365 services
- Monitor tenant health using Microsoft 365 Adoption Score
- Monitor tenant health using Microsoft 365 usage analytics
- Develop an incident response plan
- Request assistance from Microsoft

Module 8: Deploy Microsoft 365 Apps for enterprise

This module examines how to implement the Microsoft 365 Apps for enterprise productivity suite in both user-driven and centralized deployments.

Lessons

- Explore Microsoft 365 Apps for enterprise functionality
- Explore your app compatibility by using the Readiness Toolkit
- Complete a self-service installation of Microsoft 365 Apps for enterprise
- Deploy Microsoft 365 Apps for enterprise with Microsoft Configuration Manager
- Deploy Microsoft 365 Apps for enterprise from the cloud
- Deploy Microsoft 365 Apps for enterprise from a local source
- Manage updates to Microsoft 365 Apps for enterprise
- Explore the update channels for Microsoft 365 Apps for enterprise
- Manage your cloud apps using the Microsoft 365 Apps admin center

Module 9: Analyze your Microsoft 365 workplace data using Microsoft Viva Insights

This module examines the workplace analytical features of Microsoft Viva Insights, including how it works, and how it generates insights and improves collaboration within an organization.

Lessons

- Examine the analytical features of Microsoft Viva Insights
- Explore Personal insights
- Explore Team insights
- Explore Organization insights
- Explore Advanced insights

Module 10: Explore identity synchronization

This module examines identity synchronization and explores the authentication and provisioning options that can be used and the inner workings of directory synchronization.

Lessons

- Examine identity models for Microsoft 365
- Examine authentication options for the hybrid identity model
- Explore directory synchronization

Module 11: Prepare for identity synchronization to Microsoft 365

This module examines all the planning aspects that must be considered when implementing directory synchronization between on-premises Active Directory and Microsoft 365.

Lessons

- Plan your Azure Active Directory deployment
- Prepare for directory synchronization
- Choose your directory synchronization tool
- Plan for directory synchronization using Azure AD Connect
- Plan for directory synchronization using Azure AD Connect Cloud Sync

Module 12: Implement directory synchronization tools

This module examines the Azure AD Connect and Azure AD Connect Cloud Sync installation requirements, the options for installing and configuring the tools, and how to monitor synchronization services using Azure AD Connect Health.

Lessons

- Configure Azure AD Connect prerequisites
- Configure Azure AD Connect
- Monitor synchronization services using Azure AD Connect Health
- Configure Azure AD Connect Cloud Sync prerequisites
- Configure Azure AD Connect Cloud Sync

Module 13: Manage synchronized identities

This module examines how to manage user identities when you configure Azure AD Connect, how to manage users and groups in Microsoft 365 with Azure AD Connect, and how to maintain directory synchronization.

Lessons

- Manage users with directory synchronization
- Manage groups with directory synchronization
- Use Azure AD Connect Sync Security Groups to help maintain directory synchronization
- Configure object filters for directory synchronization
- Explore Microsoft Identity Manager
- Troubleshoot directory synchronization

Module 14: Manage secure user access in Microsoft 365

This module examines various password-related tasks for users and administrators, including creating and configuring password policies, configuring self-service password management, configuring multifactor authentication and implementing conditional access policies

Lessons

- Manage user passwords
- Enable pass-through authentication
- Enable multifactor authentication
- Enable passwordless sign-in with Microsoft Authenticator
- Explore self-service password management
- Explore Windows Hello for Business
- Implement Azure AD Smart Lockout
- Implement conditional access policies
- Explore Security Defaults in Azure AD
- Investigate authentication issues using sign-in logs

Module 15: Examine threat vectors and data breaches

This module examines the types of threat vectors and their potential outcomes that organizations must deal with daily and how users can enable hackers to access targets by unwittingly executing malicious content.

Lessons

- Explore today's work and threat landscape
- Examine how phishing retrieves sensitive information
- Examine how spoofing deceives users and compromises data security
- Compare spam and malware
- Examine account breaches
- Examine the elevation of privilege attacks
- Examine how data exfiltration moves data out of your tenant
- Examine how attackers delete data from your tenant
- Examine how data spillage exposes data outside your tenant
- Examine other types of attacks

Module 16: Explore the Zero Trust security model

This module examines the concepts and principles of the Zero Trust security model, as well as how Microsoft 365 supports it, and how your organization can implement it.

Lessons

- Examine the principles and components of the Zero Trust model
- Plan for a Zero Trust security model in your organization
- Examine Microsoft's strategy for Zero Trust networking
- Adopt a Zero Trust approach

Module 17: Explore security solutions in Microsoft 365 Defender

This module introduces you to several features in Microsoft 365 that can help protect your organization against cyber threats, detect when a user or computer has been compromised, and monitor your organization for suspicious activities.

Lessons

- Enhance your email security using Exchange Online Protection and Microsoft Defender for Office 365
- Protect your organization's identities using Microsoft Defender for Identity
- Protect your enterprise network against advanced threats using Microsoft Defender for Endpoint
- Protect against cyber-attacks using Microsoft 365 Threat Intelligence
- Provide insight into suspicious activity using Microsoft Cloud App Security
- Review the security reports in Microsoft 365 Defender

Module 18: Examine Microsoft Secure Score

This module examines how Microsoft Secure Score helps organizations understand what they've done to reduce the risk to their data and show them what they can do to further reduce that risk.

Lessons

- Explore Microsoft Secure Score
- Assess your security posture with Microsoft Secure Score
- Improve your secure score
- Track your Microsoft Secure Score history and meet your goals

Module 19: Examine Privileged Identity Management

This module examines how Privileged Identity Management ensures users in your organization have just the right privileges to perform the tasks they need to accomplish.

Lessons

- Explore Privileged Identity Management in Azure AD
- Configure Privileged Identity Management
- Audit Privileged Identity Management
- Control privileged admin tasks using Privileged Access Management

Module 20: Examine Azure Identity Protection

This module examines how Azure Identity Protection provides organizations the same protection systems used by Microsoft to secure identities.

Lessons

- Explore Azure Identity Protection
- Enable the default protection policies in Azure Identity Protection
- Explore the vulnerabilities and risk events detected by Azure Identity Protection
- Plan your identity investigations

Module 21: Examine Exchange Online Protection

This module examines how Exchange Online Protection (EOP) protects organizations from phishing and spoofing. It also explores how EOP blocks spam, bulk email, and malware before they arrive in users' mailboxes.

Lessons

- Examine the anti-malware pipeline
- Detect messages with spam or malware using Zero-hour auto purge
- Explore anti-spoofing protection provided by Exchange Online Protection
- Explore other anti-spoofing protection
- Examine outbound spam filtering

Module 22: Examine Microsoft Defender for Office 365

This module examines how Microsoft Defender for Office 365 extends EOP protection by filtering targeted attacks such as zero-day attacks in email attachments and Office documents, and time-of-click protection against malicious URLs.

Lessons

- Climb the security ladder from EOP to Microsoft Defender for Office 365
- Expand EOP protections by using Safe Attachments and Safe Links
- Manage spoofed intelligence
- Configure outbound spam filtering policies
- Unblock users from sending email

Module 23: Manage Safe Attachments

This module examines how to manage Safe Attachments in your Microsoft 365 tenant by creating and configuring policies and using transport rules to disable a policy from taking effect in certain scenarios.

Lessons

- Protect users from malicious attachments by using Safe Attachments
- Create Safe Attachment policies using Microsoft Defender for Office 365
- Create Safe Attachments policies using PowerShell
- Modify an existing Safe Attachments policy
- Create a transport rule to bypass a Safe Attachments policy
- Examine the end-user experience with Safe Attachments

Module 24: Manage Safe Links

This module examines how to manage Safe Links in your tenant by creating and configuring policies and using transport rules to disable a policy from taking effect in certain scenarios.

Lessons

- Protect users from malicious URLs by using Safe Links
- Create Safe Links policies using Microsoft 365 Defender
- Create Safe Links policies using PowerShell
- Modify an existing Safe Links policy
- Create a transport rule to bypass a Safe Links policy
- Examine the end-user experience with Safe Links

Module 25: Explore threat intelligence in Microsoft 365 Defender

This module examines how Microsoft 365 Threat Intelligence provides admins with evidence-based knowledge and actionable advice that can be used to make informed decisions about protecting and responding to cyber-attacks against their tenants.

Lessons

- Explore Microsoft Intelligent Security Graph
- Explore alert policies in Microsoft 365
- Run automated investigations and responses
- Explore threat hunting with Microsoft Threat Protection
- Explore advanced threat hunting in Microsoft 365 Defender
- Explore threat analytics in Microsoft 365
- Identify threat issues using Microsoft Defender reports

Module 26: Implement app protection by using Microsoft Defender for Cloud Apps

This module examines how to implement Microsoft Defender for Cloud Apps, which identifies and combats cyberthreats across all your Microsoft and third-party cloud services.

Lessons

- Explore Microsoft Defender Cloud Apps
- Deploy Microsoft Defender for Cloud Apps
- Configure file policies in Microsoft Defender for Cloud Apps
- Manage and respond to alerts in Microsoft Defender for Cloud Apps
- Configure Cloud Discovery in Microsoft Defender for Cloud Apps
- Troubleshoot Cloud Discovery in Microsoft Defender for Cloud Apps

Module 27: Implement endpoint protection by using Microsoft Defender for Endpoint

This module examines how Microsoft Defender for Endpoint helps enterprise networks prevent, detect, investigate, and respond to advanced threats by using endpoint behavioral sensors, cloud security analytics, and threat intelligence.

Lessons

- Explore Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint in Microsoft Intune
- Onboard devices in Microsoft Defender for Endpoint
- Manage endpoint vulnerabilities with Microsoft Defender Vulnerability Management
- Manage device discovery and vulnerability assessment
- Reduce your threat and vulnerability exposure

Module 28: Implement threat protection by using Microsoft Defender for Office 365

This module examines the Microsoft Defender for Office 365 protection stack and its corresponding threat intelligence features, including Threat Explorer, Threat Trackers, and Attack simulation training.

Lessons

- Explore the Microsoft Defender for Office 365 protection stack
- Investigate security attacks by using Threat Explorer
- Identify cybersecurity issues by using Threat Trackers
- Prepare for attacks with Attack simulation training

Module 29: Examine data governance solutions in Microsoft Purview

This module introduces Microsoft Purview, which is designed to meet the challenges of today's decentralized, data-rich workplace by providing a comprehensive set of solutions that help organizations govern, protect, and manage their entire data estate.

Lessons

- Explore data governance and compliance in Microsoft Purview
- Protect sensitive data with Microsoft Purview Information Protection
- Govern organizational data using Microsoft Purview Data Lifecycle Management
- Minimize internal risks with Microsoft Purview Insider Risk Management
- Explore Microsoft Purview eDiscovery solutions

Module 30: Explore archiving and records management in Microsoft 365

This module examines how Microsoft 365 supports data governance by enabling organizations to archive content by using archive mailboxes, and manage their high-value content for legal, business, or regulatory obligations by implementing records management.

Lessons

- Explore archive mailboxes in Microsoft 365
- Enable archive mailboxes in Microsoft 365
- Explore Microsoft Purview Records Management
- Implement Microsoft Purview Records Management
- Restore deleted data in Exchange Online
- Restore deleted data in SharePoint Online

Module 31: Explore retention in Microsoft 365

This module examines how data can be retained and ultimately removed in Microsoft 365 by using data retention policies and data retention labels in retention policies.

Lessons

- Explore retention by using retention policies and retention labels
- Compare capabilities in retention policies and retention labels
- Define the scope of a retention policy
- Examine the principles of retention
- Implement retention using retention policies, retention labels, and eDiscovery holds
- Restrict retention changes by using Preservation Lock

Module 32: Explore Microsoft Purview Message Encryption

This module introduces Microsoft Purview Message Encryption, an online service that's built on Microsoft Azure Rights Management and includes encryption, identity, and authorization policies to help organizations secure their email.

Lessons

- Examine Microsoft Purview Message Encryption
- Configure Microsoft Purview Message Encryption
- Define mail flow rules to encrypt email messages
- Add organizational branding to encrypted email messages
- Explore Microsoft Purview Advanced Message Encryption

Module 33: Explore compliance in Microsoft 365

This module explores the tools Microsoft 365 provides to help ensure an organization's regulatory compliance, including the Microsoft Purview compliance portal, Compliance Manager, and the Microsoft compliance score.

Lessons

- Plan for security and compliance in Microsoft 365
- Plan your beginning compliance tasks in Microsoft Purview
- Manage your compliance requirements with Compliance Manager
- Examine the Compliance Manager dashboard
- Analyse the Microsoft Compliance score

Module 34: Implement Microsoft Purview Insider Risk Management

This module examines how Microsoft Purview Insider Risk Management helps organizations minimize internal risks by enabling them to detect, investigate, and act on malicious and inadvertent activities.

Lessons

- Explore insider risk management
- Plan for insider risk management
- Explore insider risk management policies
- Create insider risk management policies
- Investigate insider risk management activities and alerts
- Explore insider risk management cases

Module 35: Implement Microsoft Purview Information Barriers

This module examines how Microsoft Purview uses information barriers to restrict communication and collaboration in Microsoft Teams, SharePoint Online, and OneDrive for Business.

Lessons

- Explore Microsoft Purview Information Barriers
- Configure information barriers in Microsoft Purview
- Examine information barriers in Microsoft Teams
- Examine information barriers in OneDrive
- Examine information barriers in SharePoint

Module 36: Explore Microsoft Purview Data Loss Prevention

This module examines the data loss prevention features in Microsoft 365 that help organizations identify, monitor, report, and protect sensitive data through deep content analysis while helping users understand and manage data risks.

Lessons

- Examine Data Loss Prevention
- Explore Endpoint data loss prevention
- Examine DLP policies
- View DLP policy results
- Explore DLP reports

Module 37: Implement Microsoft Purview Data Loss Prevention

This module examines how organizations can use Microsoft Purview Data Loss Prevention to help protect sensitive data and define the protective actions that organizations can take when a DLP rule is violated.

Lessons

- Plan to implement Microsoft Purview Data Loss Protection
- Implement Microsoft Purview's default DLP policies
- Design a custom DLP policy
- Create a custom DLP policy from a template
- Configure email notifications for DLP policies
- Configure policy tips for DLP policies

Module 38: Implement data classification of sensitive information

This module introduces you to data classification in Microsoft 365, including how to create and train classifiers, view sensitive data using Content explorer and Activity explorer, and implement Document Fingerprinting.

Lessons

- Explore data classification
- Implement data classification in Microsoft 365
- Explore trainable classifiers
- Create and retrain a trainable classifier
- View sensitive data using Content explorer and Activity explorer
- Detect sensitive information documents using Document Fingerprinting

Module 39: Explore sensitivity labels

This module examines how sensitivity labels from the Microsoft Information Protection solution let you classify and protect your organization's data, while making sure that user productivity and collaboration isn't hindered.

Lessons

- Manage data protection using sensitivity labels
- Explore what sensitivity labels can do
- Determine a sensitivity label's scope
- Apply sensitivity labels automatically
- Explore sensitivity label policies

Module 40: Implement sensitivity labels

This module examines the process for implementing sensitivity labels, including applying proper administrative permissions, determining a deployment strategy, creating, configuring, and publishing labels, and removing and deleting labels.

Lessons

- Plan your deployment strategy for sensitivity labels
- Examine the requirements to create a sensitivity label
- Create sensitivity labels
- Publish sensitivity labels
- Remove and delete sensitivity labels