MS-102 Microsoft 365 Administrator: Complete Exam Blueprint & Readiness Checklist

BY

TECHCERTGUIDE.BLOG

Contents

Introduction

The MS-102 Microsoft 365 Administrator certification validates your ability to deploy, manage, secure, and govern a Microsoft 365 environment in real-world enterprise scenarios.

This guide aligns with the official Microsoft MS-102 exam objectives as published on Microsoft Learn.

Modern organizations rely heavily on Microsoft 365 for:

- Identity and access management
- Email and collaboration
- Endpoint security
- Data protection and compliance

An administrator is no longer responsible for just “managing users.”
You are expected to understand how identity, security, compliance, and collaboration services work together as a unified platform.

This guide provides a structured framework for understanding the MS-102 exam objectives and preparing effectively.

Who This Guide Is For

This blueprint is intended for:

- IT professionals transitioning to Microsoft 365 administration
- System administrators moving from on-premises to cloud
- Security professionals working with Microsoft 365 workloads
- Support engineers preparing for a cloud-focused role
- Candidates preparing for the MS-102 certification exam

No deep development or scripting experience is required.
However, a basic understanding of IT fundamentals and Microsoft 365 services is recommended.

How to Use This Guide

This document follows Microsoft’s official exam structure and is organized into four domains:

1. Deploy and manage a Microsoft 365 tenant
2. Implement and manage Microsoft Entra ID
3. Implement and manage Microsoft Defender XDR

4. Implement and manage compliance

Each section focuses on:

- Core concepts you must understand
- Administrative responsibilities you must master
- Scenario-based areas commonly tested in the exam

This is not a lab manual or exam dump.
It is a structured blueprint designed to help you think like a Microsoft 365 administrator.

What This Guide Does Not Replace

This guide complements:

- Microsoft Learn documentation
- Hands-on lab practice
- Real-world administrative experience

Certification success requires both conceptual understanding and practical application.

Final Goal

By the end of this guide, you should be able to:

- Connect identity, security, and compliance decisions
- Select the correct Microsoft 365 solution for a scenario
- Troubleshoot administrative issues logically
- Approach the MS-102 exam with confidence

Microsoft 365 administration is not about Memorizing features. It is about understanding how the platform works as an integrated ecosystem.

This blueprint provides a structured roadmap aligned with the MS-102 exam objectives.

DOMAIN 1: Deploy and manage a Microsoft 365 Tenant (15–20%)

What This Domain Covers

This domain focuses on establishing and maintaining the foundational environment of Microsoft 365. It includes tenant configuration, domain management, service health monitoring, and Microsoft 365 Apps deployment.

Before administrators manage identity, security, or compliance, they must ensure the tenant is properly configured and operational.

Why This Domain Matters

Every configuration in Microsoft 365 starts at the tenant level. If the tenant is misconfigured, identity, licensing, and security settings will not function as expected.

Although this domain carries 15–20% of the exam weight, it provides the operational foundation for all other domains.

1.1 Deploy and Configure a Microsoft 365 Tenant

Purpose

This objective covers the foundational setup and configuration of a Microsoft 365 tenant. It focuses on preparing the organization's cloud environment before managing users, identity, security, or workloads.

This objective represents a foundational area of the MS-102 exam.

Tenant Deployment

- Create a Microsoft 365 tenant
- Understand tenant naming conventions
- Recognise the default onmicrosoft.com domain
- Identify the Tenant ID (GUID)
- Understand tenant isolation in the Microsoft cloud

Organizational Configuration

- Configure organization profile settings
- Manage company information (name, address, contact details)
- Configure release preferences (Standard vs Targeted Release)
- Understand privacy and tenant-wide policies

Administrative Setup

- Identify the Global Administrator role
- Assign additional administrative roles
- Follow least-privilege best practices
- Understand role-based access control (RBAC)

Tenant-Level Settings

- Configure security defaults
- Manage external sharing settings

- Review service availability
- Understand Organization-wide configuration scope

Key Concepts to Remember:

- Tenant = Environment
- Subscription = Product
- License = User access entitlement
- Tenant settings apply Organization-wide
- Admin roles control the scope of authority

1.2 Manage Microsoft 365 Apps

Purpose

This objective focuses on deploying, configuring, updating, and managing Microsoft 365 Apps (formerly Office 365 ProPlus) across an organization.

Administrators must understand how applications are installed, updated, secured, and maintained at scale.

This section tests practical app lifecycle management.

Deployment Methods

- Deploy Microsoft 365 Apps to users
- Understand deployment via:
    - Microsoft 365 Admin Center
    - Intune
    - Configuration Manager (SCCM)
- Understand Click-to-Run installation model
- Configure shared computer activation

Update Management

- Understand update channels:
    - Current Channel
    - Monthly Enterprise Channel
    - Semi-Annual Enterprise Channel
- Change update channel settings
- Manage version control

- Understand update deferral options

App Configuration

- Configure application settings
- Manage app policies
- Enable or turn off specific Office apps
- Configure roaming settings
- Manage cloud policy settings

App Security & Controls

- Configure macro policies
- Understand app protection policies
- Apply security baselines
- Manage trusted locations
- Understand integration with Conditional Access

Monitoring & Troubleshooting

- Monitor app installation status
- Identify activation issues
- Troubleshoot update failures
- Understand common deployment errors
- Review user activation limits

Key Concepts to Remember:

- Microsoft 365 Apps are subscription-based
- Apps update continuously via the selected channel
- Updates are cloud-managed
- Deployment strategy impacts security posture
- Shared activation is required in multi-user environments

1.3 Monitor and Troubleshoot Microsoft 365

Purpose

This objective focuses on monitoring tenant health, identifying service issues, and responding to operational problems within Microsoft 365.

Administrators must understand how to detect disruptions, Analyze usage trends, and resolve tenant-level incidents.

Monitor Service Health

- Access the Service Health dashboard
- Identify active incidents and advisories
- Understand impact scope (regional vs global)
- Interpret incident status updates
- Track resolution timelines

Interpret Message Center Notifications

- Access Message Center in Admin Center
- Identify service updates and feature changes
- Understand planned maintenance announcements
- Track roadmap changes affecting users
- Configure notification preferences

Use Usage Reports

- Access Microsoft 365 usage reports
- Review user activity metrics
- Analyze service adoption trends
- Identify inactive users
- Export usage data for analysis

Troubleshoot Tenant-Level Issues

- Identify service outages vs configuration errors
- Verify license availability
- Check domain and DNS status
- Review user access issues
- Validate admin role permissions

Perform Root Cause Analysis

- Determine whether the issue is:
    - User-level
    - License-related

    - Policy-related
    - Service-wide
- Correlate service health with user complaints
- Review configuration changes

Review Audit Logs

- Access Unified Audit Log
- Search for administrative actions
- Identify login activity
- Review configuration changes
- Investigate suspicious activity

Manage Support Requests

- Open a support ticket with Microsoft
- Provide tenant information
- Track ticket status
- Review service-level responses
- Close resolved cases

Key Concepts to Remember:

- Service health ≠ configuration error
- Message Center provides proactive awareness
- Usage reports support adoption decisions
- Audit logs provide visibility into changes
- Troubleshooting requires a structured investigation

1.4 Manage Domains

Purpose

This objective focuses on adding, verifying, and managing custom domains within a Microsoft 365 tenant.

Domains are essential for email routing, user identities, and service configuration. Proper DNS configuration ensures secure and reliable communication across Microsoft 365 services.

Add and Verify Domains

- Add a custom domain to Microsoft 365
- Verify domain ownership using TXT record
- Understand the domain verification process
- Confirm successful domain validation

Configure DNS Records

- Configure MX records for mail flow
- Configure TXT records for domain verification and SPF
- Configure CNAME records (e.g., Autodiscover)
- Configure SRV records (e.g., Teams services)
- Understand DNS propagation timing

Set Default Domain

- Change default domain for new users
- Understand the impact of default domain selection
- Configure primary SMTP domain

Update User Email Addresses

- Change user principal name (UPN)
- Update primary email address
- Configure proxy addresses
- Ensure alignment with verified domain

Validate Mail Flow

- Confirm MX record routing
- Test email delivery internally and externally
- Verify SPF configuration
- Check mail flow connectors

Troubleshoot DNS Issues

- Identify incorrect MX configuration
- Detect missing or incorrect SPF records
- Understand Autodiscover issues

- Diagnose domain verification failures
- Recognize DNS propagation delays

Key Concepts to Remember:

- Domain verification proves ownership
- DNS records control email and service routing
- Default domain affects new user creation
- UPN and primary SMTP can differ
- Incorrect DNS can cause mail disruption

Summary

Core Areas Covered:

- Deploy and configure a Microsoft 365 tenant
- Manage domains and DNS records
- Configure subscriptions and licensing
- Monitor service health and usage
- Troubleshoot tenant-level issues

What This Domain Tests:

- Understanding of tenant architecture
- Domain verification and DNS configuration
- Subscription and license management
- Admin center navigation
- Service health interpretation
- Structured troubleshooting approach

Key Concept:

Everything in Microsoft 365 begins at the tenant level. Identity, security, compliance, and collaboration all depend on proper tenant configuration.

DOMAIN 2: Implement and Manage Microsoft Entra ID (25–30%)

Domain Overview

This domain focuses on identity, authentication, access control, and role-based administration within Microsoft Entra ID (formerly Azure Active Directory).

Identity is the foundation of Microsoft 365 security. Most access, policy, and compliance decisions begin with identity configuration.

This domain carries significant exam weight and is critical for real-world administration and exam success.

2.1 Manage Identities and Roles

Users

- **Create, update, and delete users:** Create cloud-only users, modify properties, and remove accounts when no longer needed.
- **Perform bulk user operations:** Import or update multiple users using CSV or automation tools.
- **Manage user properties:** Edit display name, job title, department, UPN, contact info, etc.
- **Reset passwords:** Manually reset user passwords or enforce password change at next sign-in.
- **Unlock accounts:** Re-enable blocked sign-ins due to admin action or risk policy.
- Restore deleted users: Recover soft-deleted accounts within the retention period.
- **Manage guest users:** Invite external users (B2B collaboration) and control their access.
- **Monitor sign-in status:** Review login activity and detect failed or risky sign-ins.

Groups

- **Microsoft 365 Groups:** Collaboration groups with a mailbox, a SharePoint site, and Teams support.
- **Security Groups:** Used for access control and policy targeting.
- **Distribution Lists:** Email-only group for sending messages to multiple recipients.
- **Mail-enabled Security Groups:** Combines access control + email capability.
- **Manage group membership:** Add/remove users manually or automatically.
- **Dynamic group membership rules:** Automatically assign users/devices to groups based on attributes.

Roles & RBAC

- **Assign admin roles:** Grant built-in roles like Global Admin, Exchange Admin, etc.
- **Manage custom roles:** Create roles with specific permission sets.
- **Role-Based Access Control (RBAC):** Limit admin permissions using least-privilege **principles.**

- **Privileged Identity Management (PIM):** Enable just-in-time role activation with approval and auditing.
- **Administrative Units:** Delegate administration to specific subsets of users/groups.

2.2 Manage Authentication and Conditional Access

Purpose

Conditional Access is Microsoft Entra ID's policy engine that evaluates signals during sign-in and decides whether access should be granted, blocked, or restricted. It enforces Zero Trust by applying policies based on conditions instead of static credentials.

A Conditional Access policy follows this logic:

- If defined conditions are met
- Then specific access controls are applied

Create Conditional Access Policies

When creating a Conditional Access policy, you configure:

- Users or groups included or excluded
- Cloud apps or actions targeted
- Conditions such as:
    - Location
    - Device state
    - Sign-in risk
    - User risk
    - Client app type
    - Platform (Windows, iOS, Android, etc.)
- Access controls (grant or block)

Policies can be:

- Enabled
- Disabled
- Set to report-only mode for testing

Grant Controls

Grant controls determine what must be satisfied before access is allowed.

Common grant controls include:

- Require Multi-Factor Authentication (MFA)

- Require compliant device
- Require hybrid Azure AD joined device
- Require approved client app
- Require authentication strength

Grant logic can be configured as:

- Require all selected controls
- Require one of the selected controls

Session Controls

- Session controls manage user behavior after access is granted.

Examples include:

- Sign-in frequency enforcement
- Persistent browser session control
- Conditional Access App Control integration
- Restrict session duration

Session controls help limit exposure during active sessions.

Named Locations

- Named locations define trusted or blocked network locations.

They are used to:

- Define trusted corporate IP ranges
- Block specific countries
- Apply location-based Conditional Access policies

Device-Based Access

- Conditional Access can evaluate device status before allowing access.

Device conditions may include

- Device must be compliant (managed by Intune)
- Device must be a hybrid Azure AD joined device
- Filter devices based on attributes

This ensures only trusted and managed devices can access resources.

Risk-Based Policies

- Conditional Access integrates with Identity Protection.

Policies can enforce controls when

- User risk level is medium or high
- Sign-in risk level is medium or high

Examples:

- If sign-in risk is high → Require MFA
- If user risk is high → Require password reset

Authentication Strengths

- Authentication strengths allow enforcement of stronger authentication methods.

Examples include:

- Require phishing-resistant MFA
- Require passwordless authentication
- Require specific combinations of authentication methods

This provides more granular control than basic MFA.

Policy Evaluation Logic
Important evaluation principles:

- Multiple policies can apply at the same time
- Block access overrides grant access
- Policies should be carefully scoped
- Emergency or break-glass accounts should be excluded from restrictive policies

Key Concepts to Remember

- Conditional Access enforces Zero Trust
- Conditions determine when a policy applies
- Grant controls determine if access is allowed
- Session controls manage Behavior after access
- Risk signals enhance dynamic security

2.3 Implement Identity Protection

Purpose

Microsoft Entra Identity Protection uses Microsoft's threat intelligence and machine learning to detect and respond to identity-based risks. It continuously evaluates user Behavior and sign-in activity to determine whether an account or login attempt is potentially compromised.

There are two main types of risk evaluated:

User Risk – Indicates the likelihood that a user's account has been compromised.
Sign-in Risk – Indicates the likelihood that a specific authentication attempt is suspicious.

Identity Protection helps organizations enforce Zero Trust by applying policies based on risk signals rather than just static credentials.

Risk Detections

Risk detections identify suspicious or abnormal authentication Behavior. Examples include:

- Sign-ins from unfamiliar or high-risk locations
- Impossible travel scenarios
- Anonymous IP address usage
- Malware-linked IP addresses
- Leaked credentials detected externally

Each detection is assigned a risk level such as Low, Medium, or High. These detections contribute to overall user or sign-in risk scores.

User Risk Policies

User risk policies define what actions occur when a user's overall risk level reaches a defined threshold. These policies typically address compromised accounts.

Common actions include:

- Require password reset
- Block access until remediation
- Force secure authentication

User risk policies are designed to protect against persistent account compromise and ensure accounts are secured before further access is granted.

Sign-in Risk Policies

Sign-in risk policies apply to individual login attempts rather than the user account overall. These policies respond to real-time suspicious authentication attempts.

Possible actions include:

- Require Multi-Factor Authentication
- Block the sign-in attempt
- Allow access after additional verification

Sign-in risk policies help prevent attackers from gaining access even if credentials are valid.

Risk Remediation

Risk remediation reduces or clears a user's risk status after investigation or corrective action.

Remediation actions may include:

- Forcing a password reset
- Revoking active sessions
- Blocking the account temporarily
- Investigating suspicious activity

Once resolved, the user's risk level can return to normal if no further suspicious activity is detected.

Password Writeback

Password writeback is required in hybrid environments when cloud-based password changes must synchronize with on-premises Active Directory.

Password writeback is required when:

- Self-Service Password Reset is enabled in hybrid setups
- Cloud-based password changes must update on-prem accounts
- Without password writeback, password updates in Microsoft Entra ID would not reflect in on-premises AD.

Self-Service Password Reset (SSPR)

Self-Service Password Reset allows users to reset or unlock their accounts without administrator intervention.

Configuration includes:

- Enabling SSPR for selected users or groups
- Defining required authentication methods
- Enforcing security information registration

SSPR improves user productivity and reduces helpdesk workload. It also integrates with Identity Protection for automated remediation when accounts are marked as risky.

Key Concepts to Remember:

- User risk and sign-in risk are different but related
- Identity Protection integrates with Conditional Access
- Risk-based policies enforce dynamic security controls
- SSPR supports account recovery and remediation
- Password writeback is necessary in hybrid identity environments

2.4 Implement Hybrid Identity

Purpose

Hybrid identity connects on-premises Active Directory with Microsoft Entra ID. It allows Organizations to Synchronize identities between local infrastructure and the cloud.

Hybrid identity enables

- Single sign-on experience
- Centralized identity management
- Cloud access using on-prem credentials
- Gradual cloud transition

Microsoft Entra Connect

Microsoft Entra Connect (formerly Azure AD Connect) is the tool used to Synchronize identities between on-prem Active Directory and Microsoft Entra ID.

Key functions include:

- Synchronizing user accounts
- Synchronizing group objects
- Synchronizing passwords
- Enabling hybrid device registration

Password Hash Synchronization (PHS)

Password Hash Sync copies a hash of the on-prem password to the cloud.

Key points:

- Users authenticate directly against Microsoft Entra ID
- On-prem AD does not validate cloud sign-ins
- Simplest and most commonly used model
- Provides cloud authentication resilience

Pass-Through Authentication (PTA)

Pass-Through Authentication validates credentials against on-prem Active Directory during sign-in.

Key points:

- Authentication request is sent to on-prem agent
- Password is not stored in cloud
- Requires on-prem agent availability
- Used when password hash sync is not preferred

Federation (ADFS)

Federation uses Active Directory Federation Services (AD FS) to authenticate users.

Key points:

- Authentication redirected to on-prem federation server
- Used in complex enterprise environments
- Supports advanced authentication scenarios
- Higher infrastructure complexity

Device Synchronization

Hybrid identity can also synchronize device objects.

This enables:

- Hybrid Azure AD Join
- Device-based Conditional Access
- Compliance evaluation

Hybrid Azure AD Join

Hybrid Azure AD Join registers domain-joined devices in Microsoft Entra ID.

Benefits include:

- Seamless single sign-on
- Conditional Access enforcement
- Device compliance policies
- Centralized device visibility

Entra Connect Health

Entra Connect Health monitors hybrid identity infrastructure.

It provides:

- Sync status monitoring
- Authentication service monitoring
- Performance alerts
- Error detection

This helps administrators quickly detect sync failures or authentication disruptions.

Password Writeback

Password writeback allows password changes made in the cloud to sync back to on-prem Active Directory.

Important when:

- Using Self-Service Password Reset
- Operating hybrid identity environments

Without writeback, cloud password changes would not update on-prem credentials.

Key Concepts to Remember:

- Hybrid identity extends on-prem identity to the cloud
- PHS is the simplest and most common
- PTA validates against on-prem AD
- Federation adds complexity but flexibility
- Device hybrid join supports Conditional Access
- Connect Health monitors sync infrastructure

Summary

This domain focuses on identity, authentication, and access control.

Core Areas Covered:

- User and group management
- Role-based access control (RBAC)
- Privileged Identity Management (PIM)
- Multi-Factor Authentication (MFA)
- Conditional Access policies
- Identity Protection
- Self-Service Password Reset (SSPR)
- Hybrid identity (Entra Connect)

What This Domain Tests:

- Identity lifecycle management
- Access control logic
- Risk-based authentication
- Conditional Access design
- Hybrid identity understanding
- Delegated administration

Key Concept:

Identity is the security boundary in Microsoft 365. Most access decisions are based on identity signals and policy enforcement.

DOMAIN 3: Implement and Manage Microsoft Defender XDR (35–40%)

Domain Overview
This domain focuses on implementing and managing Microsoft Defender XDR security solutions across Microsoft 365 workloads.

It covers protection, detection, investigation, and response capabilities across:

- Email
- Identity
- Endpoints
- Cloud applications

This domain carries the highest exam weight and is heavily scenario-based.

3.1 Microsoft Defender for Office 365

Purpose
Protect Exchange Online and collaboration workloads from phishing, malware, impersonation, and advanced email-based threats.

Anti-Spam Policies
Control inbound and outbound spam filtering.

- Configure spam confidence levels (SCL)
- Configure outbound spam protection
- Manage quarantine policies
- Allow/block senders and domains

Exam focus: Know the difference between spam filtering and anti-phishing protection.

Anti-Malware Policies
Detect and block malicious files in email.

- Configure malware filtering settings
- Block specific file types
- Configure notification settings

Exam focus: Understand attachment-based threat prevention.

Safe Links
Protect users from malicious URLs in emails and Teams.

- Enable time-of-click URL protection

- Rewrite and scan URLs
- Apply policy to specific users/groups

Exam focus: Safe Links protects URLs, not attachments.

Safe Attachments

Protect against zero-day malware in attachments.

- Scan attachments in a sandbox environment
- Use dynamic delivery to reduce delays
- Block or monitor suspicious files

Exam focus: Safe Attachments = attachment sandboxing.

Anti-Phishing Policies

Protect against impersonation and spoofing attacks.

- Configure user and domain impersonation protection
- Enable spoof intelligence
- Protect high-value accounts (VIPs)

Exam focus: Know the difference between spoof protection and impersonation protection.

Mail Flow Rules (Transport Rules)

Apply conditions and actions to email messages.

- Create conditional email routing rules
- Apply disclaimers
- Enforce compliance policies
- Block or redirect messages

Exam focus: Understand when to use mail flow rules vs security policies.

Threat Explorer

Investigate and Analyze email threats.

- Search by sender, URL, IP, file hash
- Review attack timeline
- Investigate impacted users

Exam focus: Threat Explorer = investigation tool, not prevention.

Attack Simulation Training

Simulate phishing attacks to test user awareness.

- Run phishing campaigns

- Track user responses
- Identify risky users

Exam focus: Awareness tool, not technical protection control.

3.2 Microsoft Defender for Endpoint

Purpose

Microsoft Defender for Endpoint protects organizational devices against advanced threats. It provides detection, investigation, and automated response capabilities across endpoints such as Windows devices.

It integrates with Microsoft Defender XDR and Conditional Access to strengthen the security posture.

Onboard Devices

Onboarding connects devices to Microsoft Defender for Endpoint so they can be monitored and protected.

Key points:

- Onboard Windows devices using:
  - Intune
  - Group Policy
  - Configuration Manager
  - Manual script
- Once onboarded, devices send telemetry to Defender
- Device health and threat status become visible in the portal

Exam focus: Understand that onboarding is required before monitoring and protection.

Device Compliance

Device compliance evaluates whether a device meets organizational security standards.

Compliance may include:

- Antivirus enabled
- OS up to date
- Encryption enabled
- Security settings configured

Defender integrates with Intune so that device compliance can be enforced through Conditional Access.

Exam focus: Know the relationship between device compliance and Conditional Access policies.

Endpoint Detection and Response (EDR)

EDR detects suspicious Behavior and advanced attacks on devices.

Capabilities include:

- Behavioral detection of threats
- Real-time alert generation
- Automated investigation
- Response actions such as isolating a device

EDR focuses on post-breach detection and response.

Exam focus: Understand EDR is detection and response, not just prevention.

Device Risk Level

Each onboarded device is assigned a risk level based on detected threats.

Risk levels may be:

- Low
- Medium
- High

This risk level can be used in Conditional Access policies to:

- Block access from risky devices
- Require remediation before access

Exam focus: Device risk integrates with Conditional Access for dynamic security enforcement.

Threat Analytics

Threat analytics provides insights into active attack campaigns and vulnerabilities.

It helps administrators:

- Understand exposure to emerging threats
- Review recommended actions
- Assess potential impact on devices

Threat analytics is informational and strategic rather than real-time blocking.

Exam focus: Understand how analytics supports decision-making and remediation planning.

Remediation Actions

Defender allows administrators to respond to threats directly from the portal.

Common remediation actions:

- Isolate the device from the network
- Run an antivirus scan
- Collect the investigation package
- Restrict app execution
- Remove malicious files

These actions help contain threats and prevent lateral movement.

Exam focus: Know which actions are containment, investigation, or prevention.

Key Concepts to Remember

- Defender for Endpoint protects devices
- Onboarding enables monitoring
- EDR detects suspicious Behavior
- Device risk affects access control
- Remediation actions contain threats

3.3 Microsoft Defender for Identity

Purpose

Microsoft Defender for Identity monitors on-premises Active Directory environments to detect identity-based attacks. It focuses on identifying suspicious activities related to user accounts, domain controllers, and authentication traffic.

It is primarily relevant in hybrid environments where on-prem AD is integrated with Microsoft Entra ID.

Identity Threat Monitoring

Defender for Identity continuously monitors:

- Domain controller traffic
- Authentication requests
- Account Behavior patterns
- Privileged account usage

It Analyzes signals to detect abnormal identity Behavior, such as:

- Unusual privilege escalation

- Suspicious lateral movement
- Reconnaissance activity inside the network

Exam focus: Understand that Defender for Identity protects on-prem Active Directory identities, not just cloud accounts.

Suspicious Activity Detection

The solution detects advanced identity attacks, including:

- Pass-the-Hash attacks
- Pass-the-Ticket attacks
- Golden Ticket attacks
- Brute force attempts
- Reconnaissance scanning
- Unusual administrative activity

These detections are based on Behavioral analytics and known attack techniques.

Exam focus: Know that Defender for Identity specializes in identity-based attack detection within hybrid environments.

Alerts Investigation

When suspicious activity is detected, Defender generates alerts that can be investigated in the Microsoft Defender portal.

Administrators can:

- Review alert details
- Identify impacted users
- Trace attack timeline
- Correlate with other Defender alerts
- Take remediation actions

Alerts from Defender for Identity are often correlated into broader incidents within Microsoft Defender XDR.

Exam focus: Understand that alerts are centralized in the Defender portal and correlated across workloads.

Key Concepts to Remember:

- Defender for Identity protects on-prem AD
- It detects identity-based attacks

- It integrates with Defender XDR
- Alerts are investigated in the Defender portal
- It is especially relevant in a hybrid environment

3.4 Microsoft Defender for Cloud Apps

Purpose

Microsoft Defender for Cloud Apps provides visibility and control over cloud application usage. It helps Organizations detect risky cloud services, monitor user Behavior, and enforce security policies across SaaS applications.

It is commonly used to manage shadow IT and enforce access control in cloud environments.

Cloud App Discovery

Cloud app discovery identifies applications being accessed by users, including unsanctioned or risky cloud services.

Key capabilities include:

- Discover shadow IT applications
- Analyze traffic logs
- Assess risk level of cloud apps
- Identify high-risk or non-compliant services

Each discovered app is assigned a risk score based on security posture, compliance certifications, and industry reputation.

Exam focus: Understand that Cloud App Discovery provides visibility into unsanctioned cloud app usage.

App Governance

App governance controls how users interact with approved cloud applications.

It allows administrators to:

- Monitor app permissions
- Detect over-permissioned applications
- Identify suspicious app Behavior
- Remove risky OAuth app access

This is especially important for third-party applications connected to Microsoft 365.

Exam focus: Know that app governance focuses on application-level access control and risk monitoring.

Session Policies

Session policies provide real-time control over user activity in cloud applications.

Examples include:

- Monitor user sessions
- Block file downloads
- Restrict copy or print actions
- Enforce conditional access session control

Session policies allow granular control during active sessions.

Exam focus: Understand that session policies control Behavior after authentication.

Conditional Access Integration

Defender for Cloud Apps integrates with Conditional Access to enforce real-time access decisions.

Integration enables:

- Real-time session monitoring
- Conditional Access App Control
- Blocking risky sessions
- Applying additional restrictions during access

Example:

If a user signs in from a risky location, Conditional Access can route the session through Defender for Cloud Apps for monitoring and restriction.

Exam focus: Understand that Conditional Access and Cloud Apps work together to enforce session-level protection.

Key Concepts to Remember:

- Cloud App Discovery identifies shadow IT
- App governance controls app-level permissions
- Session policies manage real-time activity
- Conditional Access integration enhances enforcement
- Defender for Cloud Apps focuses on SaaS visibility and control

3.5 Microsoft Defender XDR Portal

Purpose

The Microsoft Defender XDR portal is the centralized security management and

investigation platform for Microsoft 365 security workloads. It correlates signals from email, endpoints, identity, and cloud apps into unified incidents.

It allows administrators to detect, investigate, and respond to security threats from a single interface.

Incident Investigation

Incidents group multiple related alerts into a single investigation view.

Key capabilities:

- View correlated alerts across workloads
- Analyze attack timeline
- Identify impacted users and devices
- Review evidence and entities involved
- Take remediation actions

Incidents help reduce alert fatigue by consolidating related threats into a single case.

Exam focus: Understand that incidents aggregate alerts from multiple Defender services.

Advanced Hunting

Advanced Hunting allows administrators to query security data using Kusto Query Language (KQL).

It enables:

- Searching across email, endpoints, identities, and cloud apps
- Investigating suspicious activity
- Correlating events across workloads
- Creating custom detection queries

Advanced Hunting is used for deeper investigation beyond standard alerts.

Exam focus: Know that Advanced Hunting is for investigation, not policy configuration.

Alerts and Incidents

Alerts are triggered when suspicious or malicious activity is detected.

Key points:

- Alerts originate from Defender for Office 365, Endpoint, Identity, or Cloud Apps
- Multiple alerts can form a single incident
- Each alert includes a severity level

- Alerts include recommended actions

Understanding the difference:

- Alert = Individual detection
- Incident = Collection of related alerts

Exam focus: Know how alerts are correlated into incidents.

Secure Score (Defender & Identity)

Secure Score measures an organization's security posture based on configured protections.

It provides:

- Score percentage
- Recommended improvement actions
- Risk reduction impact
- Priority ranking

Defender Secure Score focuses on threat protection controls.
Identity Secure Score focuses on identity security configuration.

Exam focus: Understand Secure Score provides recommendations, not enforcement.

Threat Analytics

Threat Analytics provides insights into active attack campaigns and emerging threats.

It helps administrators:

- Understand attack techniques
- Assess exposure to vulnerabilities
- Review recommended mitigation steps

Threat analytics supports proactive security planning.

Exam focus: Know that Threat Analytics provides intelligence and guidance, not direct enforcement.

Key Concepts to Remember:

- Defender XDR centralizes security management
- Incidents group related alerts
- Advanced Hunting uses KQL
- Secure Score measures posture improvement
- Threat Analytics provides intelligence insights

Summary

This is the largest and most heavily weighted domain. It focuses on threat protection, detection, and response.

Core Areas Covered:

- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Incident investigation and Advanced Hunting
- Secure Score
- Threat analytics

What This Domain Tests:

- Email threat protection
- Endpoint risk evaluation
- Identity-based attack detection
- Cloud app governance
- Incident correlation
- Response and remediation actions

Key Concept:

Defender XDR integrates signals across workloads to provide unified threat detection and response.

DOMAIN 4: Implement and Manage Compliance (15–20%)

This domain focuses on implementing and managing compliance, data protection, and information governance features within Microsoft 365.

It covers Microsoft Purview capabilities that help organizations:

- Protect sensitive data
- Meet regulatory requirements
- Manage data lifecycle
- Investigate and respond to compliance issues

4.1 Microsoft Purview Data Lifecycle Management

Purpose

Data Lifecycle Management in Microsoft Purview helps Organizations control how long data is retained and when it is deleted. It ensures compliance with legal, regulatory, and Organizational data retention requirements.

It applies across:

- Exchange Online
- SharePoint Online
- OneDrive
- Microsoft Teams

Retention Policies

Retention policies apply retention settings to entire locations, such as mailboxes or SharePoint sites.

They allow administrators to:

- Retain content for a specified period
- Delete content after a defined period
- Retain and then delete content automatically

Key characteristics:

- Applied broadly to users or sites
- Work automatically without user interaction
- Can retain or delete content

Exam focus: Understand retention policies apply at the workload/location level.

Retention Labels

Retention labels are applied at the item level (email or document).

They allow administrators to:

- Retain specific items for defined periods
- Mark items as records
- Trigger disposition review
- Apply retention based on content classification

Retention labels can be:

- Manually applied by users

- Automatically applied based on rules

Exam focus: Know the difference between retention policies (location-wide) and retention labels (item-level).

Records Management

Records management ensures important documents or emails cannot be altered or deleted inappropriately.

When content is declared as a record:

- Editing may be restricted
- Deletion may be blocked
- Audit tracking is enabled

Types of records:

- Standard records
- Regulatory records (stricter protection)

Exam focus: Understand that records management prevents modification or deletion of critical content.

Disposition Review

Disposition review is the process of reviewing content before permanent deletion.

It allows designated reviewers to:

- Approve deletion
- Extend retention period
- Document justification

Disposition review ensures:

- Controlled deletion
- Compliance validation
- Legal oversight

Exam focus: Know that disposition review is tied to retention labels, not general retention policies.

Key Concepts to Remember:

- Retention policies apply to locations
- Retention labels apply to individual items
- Records management protects critical content

- Disposition review adds approval before deletion
- Lifecycle management controls data retention and deletion timing

4.2 Microsoft Purview Information Protection

Purpose

Microsoft Purview Information Protection helps Organizations classify, label, and protect sensitive data across Microsoft 365 workloads. It ensures that confidential information is properly identified and secured using labelling and encryption controls.

It applies to:

- Exchange Online
- SharePoint Online
- OneDrive
- Microsoft Teams
- Microsoft 365 Apps (Word, Excel, Outlook, etc.)

Sensitivity Labels

Sensitivity labels classify and protect content based on its sensitivity level.

Labels can:

- Add visual markings (headers, footers, watermarks)
- Apply encryption
- Restrict access
- Control sharing
- Enforce protection settings

Common label examples:

- Public
- Internal
- Confidential
- Highly Confidential

Sensitivity labels can be applied to:

- Emails
- Documents
- Containers (Teams, SharePoint sites, Microsoft 365 Groups)

Exam focus: Understand that sensitivity labels protect and classify content.

Label Policies

Label policies define who can see and use sensitivity labels.

They control:

- Which users or groups receive labels
- Default label settings
- Mandatory labelling requirements
- User justification for label downgrade

Label policies publish labels to users.

Exam focus: Know that label policies make sensitivity labels available to users.

Encryption Settings

Encryption protects content from unAuthorized access.

When encryption is applied:

- Only Authorized users can open the content
- Forwarding or printing may be restricted
- Access may expire after a defined time

Encryption settings can:

- Restrict access to specific users or groups
- Prevent external sharing
- Control permissions such as view-only

Exam focus: Understand how encryption is applied through sensitivity labels.

Auto-Labelling

Auto-labelling automatically applies sensitivity labels based on defined conditions.

Conditions may include:

- Sensitive information types (e.g., credit card numbers)
- Keywords
- Content inspection rules

Auto-labelling reduces reliance on manual user labelling.

Exam focus: Know that auto-labelling applies labels automatically based on content detection.

Label Publishing

Label publishing is the process of assigning sensitivity labels to specific users or groups.

It determines:

- Which labels users can select
- Label priority order
- Default labelling Behavior

Without publishing, labels are not visible to users.

Exam focus: Understand that labels must be published to be used.

Key Concepts to Remember:

- Sensitivity labels classify and protect content
- Label policies publish labels to users
- Encryption is configured through labels
- Auto-labelling applies protection automatically
- Labels can protect both content and containers

4.3 Data Loss Prevention (DLP)

Purpose

Data Loss Prevention (DLP) helps prevent sensitive information from being shared, transmitted, or exposed inappropriately. It monitors and controls data across Microsoft 365 services to reduce the risk of accidental or intentional data leakage.

DLP applies across:

- Exchange Online
- SharePoint Online
- OneDrive
- Microsoft Teams
- Endpoint devices

DLP Policies

A DLP policy defines how sensitive information is detected and what actions are taken.

A policy includes:

- Locations where the policy applies
- Conditions that detect sensitive information

- Actions taken when conditions are met

Policies can be created using:

- Built-in templates (e.g., financial data, personal data)
- Custom rules

Exam focus: Understand that DLP policies define the overall framework for protecting sensitive data.

DLP Rules

DLP rules are the specific conditions and actions inside a policy.

A rule defines:

- What to detect (e.g., credit card numbers)
- When to trigger (e.g., shared externally)
- What action to take

Common actions include:

- Block sharing
- Send alert
- Restrict access
- Display policy tip to the user

Exam focus: Know that rules are the enforcement logic inside a DLP policy.

DLP Alerts

DLP alerts notify administrators when a policy rule is triggered.

Alerts can:

- Notify administrators
- Notify compliance teams
- Appear in the compliance portal

Alerts provide visibility into:

- Policy violations
- Repeated user Behavior
- High-risk data exposure

Exam focus: Understand that alerts provide monitoring and investigation visibility.

Endpoint DLP

Endpoint DLP extends DLP protection to Windows devices.

It allows administrators to:

- Block copying sensitive data to USB drives
- Prevent printing sensitive documents
- Restrict copying to the clipboard
- Monitor file transfers

Endpoint DLP protects data even when it leaves cloud services.

Exam focus: Know that Endpoint DLP protects data on devices, not just in cloud services.

DLP for Exchange, SharePoint, and Teams

DLP policies can apply across collaboration services.

Exchange Online:

- Scan emails for sensitive data
- Block sending to external recipients
- Apply policy tips

SharePoint and OneDrive:

- Prevent external sharing
- Restrict document access
- Block download of sensitive files

Microsoft Teams:

- Monitor chat messages
- Block sensitive content in conversations
- Apply DLP to shared files

Exam focus: Understand that DLP protects data across email, files, and chat.

Key Concepts to Remember:

- DLP prevents sensitive data leakage
- Policies define protection scope
- Rules define enforcement conditions
- Alerts provide visibility

- Endpoint DLP extends protection to devices
- DLP applies across Exchange, SharePoint, OneDrive, and Teams

4.4 Insider Risk Management

Purpose

Insider Risk Management in Microsoft Purview helps detect, investigate, and respond to potentially risky activities performed by internal users. It focuses on identifying Behavior that may lead to data leakage, compliance violations, or security incidents.

Unlike external threat protection, Insider Risk Management focuses on risks originating from trusted internal users.

Insider Risk Policies

Insider risk policies define what user activities should be monitored and how risk is evaluated.

Policies can be based on templates such as:

- Data leaks
- Data theft by departing employees
- Security policy violations
- Regulatory compliance violations

When configuring a policy, administrators define:

- Users or groups to monitor
- Indicators to evaluate
- Risk thresholds
- Alert severity levels

Exam focus: Understand that insider risk policies define monitoring scope and risk scoring logic.

Risk Indicators

Risk indicators are Behavioral signals that suggest potentially risky activity.

Examples include:

- Downloading large volumes of files
- Copying files to external storage
- Sharing sensitive data externally
- Accessing files outside normal working hours

- Repeated policy violations

These indicators are evaluated and assigned risk levels, such as:

- Low
- Medium
- High

Risk scoring helps determine when alerts are generated.

Exam focus: Know that risk indicators measure Behavioral patterns, not single isolated actions.

Alert Investigation

When risky activity exceeds defined thresholds, Insider Risk Management generates alerts.

Administrators can:

- Review user activity timeline
- Correlate related events
- Assess severity and impact
- Escalate or resolve alerts

Alerts provide contextual information such as:

- Files accessed
- Actions taken
- Risk score trend

Investigation tools help determine whether the Behavior is malicious, accidental, or acceptable.

Exam focus: Understand that alert investigation supports compliance review and internal risk assessment.

Key Concepts to Remember:

- Insider Risk Management monitors internal Behavior
- Policies define monitoring rules
- Risk indicators evaluate Behavioral signals
- Alerts trigger when risk thresholds are exceeded
- Investigation tools provide contextual evidence

4.5 eDiscovery and Audit

Purpose

eDiscovery and Audit in Microsoft Purview help Organizations search, preserve, and investigate data across Microsoft 365 workloads. These tools are commonly used for legal investigations, regulatory compliance, and internal reviews.

They provide visibility into user activity and stored content.

Content Search

Content Search allows administrators to search for emails, documents, and Teams messages across Microsoft 365.

It can search:

- Exchange mailboxes
- SharePoint sites
- OneDrive accounts
- Microsoft Teams messages

Administrators can:

- Use keywords and filters
- Preview search results
- Export results for further review

Exam focus: Understand that Content Search is the foundational search tool used before advanced case management.

eDiscovery (Standard)

eDiscovery (Standard) allows administrators to manage legal investigations.

It enables:

- Creating cases
- Performing content searches within cases
- Exporting results
- Placing content on hold

Standard eDiscovery is suitable for basic investigation needs.

Exam focus: Know that eDiscovery (Standard) builds on Content Search with case management and holds.

eDiscovery (Premium)

eDiscovery (Premium) provides advanced investigation capabilities.

Additional features include:

- Advanced data collection
- Custodian management
- Review sets
- Analytics and filtering
- Legal hold management

Premium is used for complex or large-scale investigations.

Exam focus: Understand that Premium offers advanced analytics and workflow tools beyond Standard.

Audit Logs

Audit logs record user and administrator activity within Microsoft 365.

They track actions such as:

- File access and modification
- Email sending and deletion
- Admin configuration changes
- Permission changes

Audit logs support:

- Security investigations
- Compliance reporting
- Activity monitoring

Exam focus: Know that audit logs track activity, not content.

Litigation Hold

Litigation hold preserves mailbox content for legal purposes.

When enabled:

- Deleted content is retained
- Content cannot be permanently removed
- Retention applies even if the user deletes data

Litigation hold applies primarily to Exchange mailboxes.

Exam focus: Understand that litigation hold prevents deletion during legal proceedings.

Case Management

Case management allows administrators to organize investigations.

It provides:

- Centralized case workspace
- Search and hold management
- Role-based access for investigators
- Documentation of investigation actions

Cases help maintain structured and secure investigation processes.

Exam focus: Understand that cases organise eDiscovery investigations and preserve evidence.

Key Concepts to Remember:

- Content Search finds data
- eDiscovery manages investigations
- Premium adds advanced review capabilities
- Audit logs track actions
- Litigation hold preserves mailbox content
- Case management organises investigations

4.6 Microsoft 365 Backup (Newer Objective)

Purpose

Microsoft 365 Backup provides native backup and recovery capabilities for Microsoft 365 workloads. It helps organizations protect against accidental deletion, ransomware, and data corruption.

This objective focuses on understanding backup capabilities and recovery scenarios rather than configuration depth.

Backup Overview

Microsoft 365 Backup focuses on protecting core workloads such as:

- Exchange Online mailboxes
- SharePoint Online sites
- OneDrive accounts

Key characteristics:

- Provides backup and point-in-time recovery
- Supports fast restoration
- Helps protect against accidental or malicious deletion
- Complements retention and compliance policies

Important concept:

Retention policies and litigation hold are not backups.
Backup provides a separate recovery capability beyond retention logic.

Exam focus: Understand the difference between retention and backup.

Recovery Options

Backup solutions allow restoration of:

- Entire mailbox
- Entire SharePoint site
- Individual items
- Specific point-in-time versions

Recovery may include:

- Restore to original location
- Restore to the alternate location
- Recover deleted items

Administrators must understand which recovery option fits the scenario.

Exam focus: Identify the correct restore method based on the data loss situation.

Restore Data Scenarios

Common recovery scenarios include:

Accidental Deletion

- User deletes important emails or files
- Administrator restores from backup

Ransomware Attack

- Files encrypted or modified
- Restore the clean version from the backup

Data Corruption

- Files damaged due to sync error

- Restore previous version

User Offboarding

- Recover the former employee's data if required

Exam focus: Select appropriate recovery action for the scenario.

Key Concepts to Remember:

- Backup protects against data loss
- Retention policies manage lifecycle, not recovery
- Restore can be item-level or workload-level
- Backup supports business continuity
- Backup complements compliance controls

Summary

This domain focuses on data protection, governance, and regulatory compliance.

Core Areas Covered:

- Data Lifecycle Management
- Retention policies and labels
- Records management
- Sensitivity labels and encryption
- Data Loss Prevention (DLP)
- Insider Risk Management
- eDiscovery and audit
- Microsoft 365 Backup

What This Domain Tests:

- Protecting sensitive information
- Managing data retention
- Investigating internal risks
- Preserving legal evidence
- Selecting the correct compliance solution

Key Concept:

Compliance controls govern how data is classified, retained, protected, and investigated.

Additional Cross-Domain Skills

These topics are not listed as a separate exam domain, but they appear repeatedly in scenario-based questions throughout the exam.

Understanding how these tools and concepts connect across workloads is essential for real-world administration and exam readiness.

These appear across multiple domains:

Microsoft Graph PowerShell

Purpose
Microsoft Graph PowerShell is used to automate and manage Microsoft 365 and Microsoft Entra ID through scripting.

It replaces older modules like AzureAD and MSOnline.

Common Administrative Uses

- Bulk user creation
- Bulk license assignment
- Managing group membership
- Reporting user properties
- Automating repetitive admin tasks

Why It Matters for MS-102

- You may see scenarios involving bulk operations
- You should understand that automation is available
- You should know Graph PowerShell is the modern management interface

Exam Focus

You are not required to memorize cmdlets.
You must understand:

- Graph PowerShell is used for automation
- It manages Entra ID, licensing, and directory objects
- It supports large-scale administrative tasks

Exchange Online Administration

Purpose
Exchange Online manages email, mail flow, and mailbox configuration.

Common Administrative Areas

- Mailbox management
- Mail flow rules (transport rules)
- Anti-spam policies
- Anti-phishing policies
- Mailbox permissions
- Shared mailboxes

Why It Matters for MS-102

Exchange Online is heavily tested under:

- Defender for Office 365
- DLP
- eDiscovery
- Litigation Hold

Exam Focus

Understand:

- Mail flow rules apply conditions and actions to messages
- Anti-spam differs from anti-phishing
- Litigation Hold preserves mailbox data
- Mailbox permissions control delegate access

SharePoint Online Administration

Purpose
SharePoint Online manages document storage and collaboration.

Common Administrative Areas

- Site creation and management
- Sharing controls
- External access settings
- Storage limits
- Site-level permissions

Why It Matters for MS-102

SharePoint is involved in:

- DLP

- Sensitivity labels
- Retention policies
- Insider risk
- External sharing scenarios

Exam Focus

Understand:

- Sharing settings can be tenant-wide or site-level
- Sensitivity labels can apply to SharePoint sites
- DLP policies protect SharePoint documents

Teams Administration

Purpose
Microsoft Teams manages collaboration, meetings, and messaging.

Common Administrative Areas

- Messaging policies
- Meeting policies
- External access
- Guest access
- App permissions

Why It Matters for MS-102

Teams is tested under:

- DLP
- Conditional Access
- Defender for Office 365
- Sensitivity labels (container-level protection)

Exam Focus

Understand:

- External access vs guest access
- DLP applies to Teams chat
- Sensitivity labels can protect Teams

License Management

Purpose
Licenses determine which services users can access.

Common Administrative Tasks

- Assign licenses to users
- Remove licenses
- View service plans within licenses
- Monitor license availability

Important Concept

License = Access entitlement
Subscription = Purchased product
Tenant = Environment

Why It Matters for MS-102

Many scenario questions involve:

- User cannot access Teams
- Mailbox not provisioned
- Service disabled due to license removal

Exam Focus

Understand:

- Assigning a license activates services
- Removing a license may remove service access
- Service plans can be turned on or off individually

Group-Based Licensing

Purpose
Group-based licensing automatically assigns licenses to users based on group membership.

How It Works

- Assign license to a security group
- Users added to the group automatically receive a license
- Users removed from the group lose their license

Why It Matters

- Reduces manual license management
- Supports automation and scalability
- Frequently tested in identity scenarios

Exam Focus

Understand:

- It simplifies license management
- Works with security groups
- Supports service plan control

Secure Score

Purpose
Secure Score measures the organization's security posture.

It provides:

- Score percentage
- Recommended improvements
- Risk reduction insights

There are different Secure Scores:

- Microsoft Defender Secure Score
- Identity Secure Score

Important Concept

Secure Score provides recommendations.
It does not automatically enforce security changes.

Exam Focus

Understand:

- Secure Score identifies improvement areas
- It measures configuration strength
- It is used for posture assessment

Admin Center Navigation

Purpose
Microsoft 365 administration is divided across multiple portals.

Main Portals

- Microsoft 365 Admin Center

- Microsoft Entra Admin Center
- Microsoft Defender Portal
- Microsoft Purview Compliance Portal
- Exchange Admin Center
- SharePoint Admin Center
- Teams Admin Center

Why It Matters

Exam questions may require knowing:

- Where a setting is configured
- Which portal controls specific features

Exam Focus

Understand:

- Identity settings are in Entra
- Threat protection is in Defender
- Compliance settings are in Purview
- Tenant settings are in M365 Admin Center

Troubleshooting Access Issues

Purpose
Troubleshooting scenarios combine multiple domains.

Common Causes of Access Problems

- License not assigned
- Conditional Access blocking access
- MFA requirement not met
- Device not compliant
- User blocked from sign-in
- Domain or DNS misconfiguration

Structured Troubleshooting Approach

1. Verify user account status
2. Verify license assignment
3. Review Conditional Access policies

4. Check device compliance
5. Review sign-in logs
6. Check service health

Why It Matters

MS-102 includes scenario-based questions requiring logical troubleshooting.

Exam Focus

Understand:

- Access issues often involve identity + licensing + policies
- Sign-in logs provide diagnostic information
- Conditional Access is a common blocking cause

Final Perspective

These cross-domain skills:

- Connect identity, security, and compliance
- Appear across multiple exam objectives
- Improve scenario-based reasoning

They are not separate objectives, but they strengthen your ability to answer complex administrative questions.

Final Exam Readiness Checklist

Use this checklist to evaluate whether you are fully prepared for the MS-102 exam.

Confidence across these areas indicates strong readiness for the MS-102 exam:

DOMAIN 1 – Deploy and Manage a Microsoft 365 Tenant

✓ I understand what a Microsoft 365 tenant is and how it is structured
✓ I can add and verify custom domains
✓ I understand DNS records (MX, TXT, CNAME, SRV)
✓ I can differentiate tenant vs subscription vs license
✓ I know how to monitor Service Health and Message Center
✓ I can interpret usage reports
✓ I understand the tenant-level troubleshooting workflow

DOMAIN 2 – Implement and Manage Microsoft Entra ID

✓ I can create, manage, and restore users
✓ I understand Microsoft 365 Groups vs Security Groups
✓ I can assign and manage admin roles
✓ I understand Role-Based Access Control (RBAC)
✓ I can configure and troubleshoot MFA
✓ I can design Conditional Access policies
✓ I understand user risk vs sign-in risk
✓ I understand Identity Protection basics
✓ I can explain Password Hash Sync vs PTA vs Federation
✓ I understand group-based licensing

DOMAIN 3 – Implement and Manage Microsoft Defender XDR

✓ I understand Safe Links vs Safe Attachments
✓ I can configure anti-phishing and anti-spam policies
✓ I understand device onboarding for Defender for Endpoint
✓ I know how device risk integrates with Conditional Access
✓ I understand identity-based threat detection
✓ I can differentiate alert vs incident
✓ I understand the Secure Score purpose
✓ I know when to use Threat Explorer
✓ I understand remediation actions (isolate device, reset password, revoke sessions)

DOMAIN 4 – Implement and Manage Compliance

✓ I understand retention policies vs retention labels
✓ I know how records management works
✓ I understand sensitivity labels and encryption
✓ I can differentiate DLP vs sensitivity labels
✓ I understand Insider Risk Management basics
✓ I can explain Content Search vs eDiscovery
✓ I understand audit logs and investigation workflow
✓ I understand litigation hold
✓ I understand the difference between retention and backup

Cross-Domain Administrative Confidence

✓ I can troubleshoot access issues logically
✓ I can identify license-related access problems
✓ I understand which admin center controls which settings

✓ I understand how identity, security, and compliance interact

✓ I can choose the correct Microsoft 365 tool for a scenario

Final Self-Assessment

If you can:

- Explain each domain without notes
- Solve scenario-based problems logically
- Identify the correct tool for each situation
- Connect identity, security, and compliance decisions

You are well prepared to attempt the MS-102 exam.