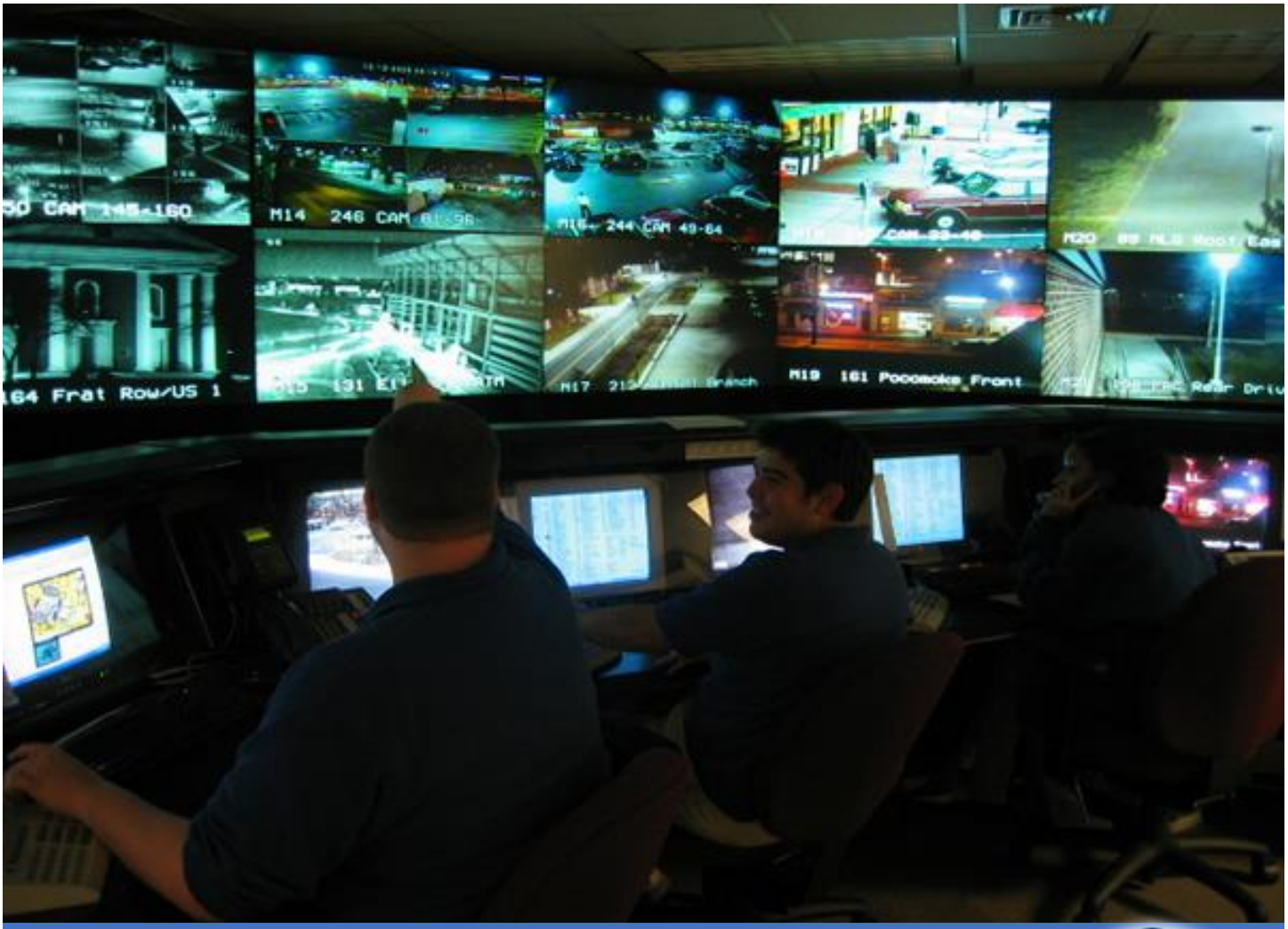


Microsoft 365 Certified: Security Administrator Associate

Microsoft 365 Security Administrators proactively secure Microsoft 365 enterprise and hybrid environments, implement and manage security and compliance solutions, respond to threats, and enforce data governance

Brought to you by

Knights Innovation Support Centre (Pty) Ltd

Microsoft Imagine Academy

Program Member

Microsoft 365 Certified: Security Administrator Associate

Microsoft 365 Security Administrators proactively secure Microsoft 365 enterprise and hybrid environments, implement and manage security and compliance solutions, respond to threats, and enforce data governance.

There are 4 areas of training and understanding required in preparation for this certification.

Exam Title	**Course Title (developing areas of training and understanding)**
Microsoft 365 Certified: **Security Administrator Associate**	Managing Microsoft 365 Identity and Access
	Implementing Microsoft 365 Threat Protection
	Implementing Microsoft 365 Information Protection
	Administering Microsoft 365 Built-in Compliance

Candidates for this exam implement, manage, and monitor security and compliance solutions for Microsoft 365 and hybrid environments. The Microsoft 365 Security Administrator proactively secures Microsoft 365 enterprise environments, responds to threats, performs investigations, and enforces data governance.

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 ensures that the solutions comply with the policies and regulations of the organization.

Candidates for this exam are familiar with Microsoft 365 workloads and have strong skills and experience with identity protection, information protection, threat protection, security management, and data governance. This role focuses on the Microsoft 365 environment and includes hybrid environments.

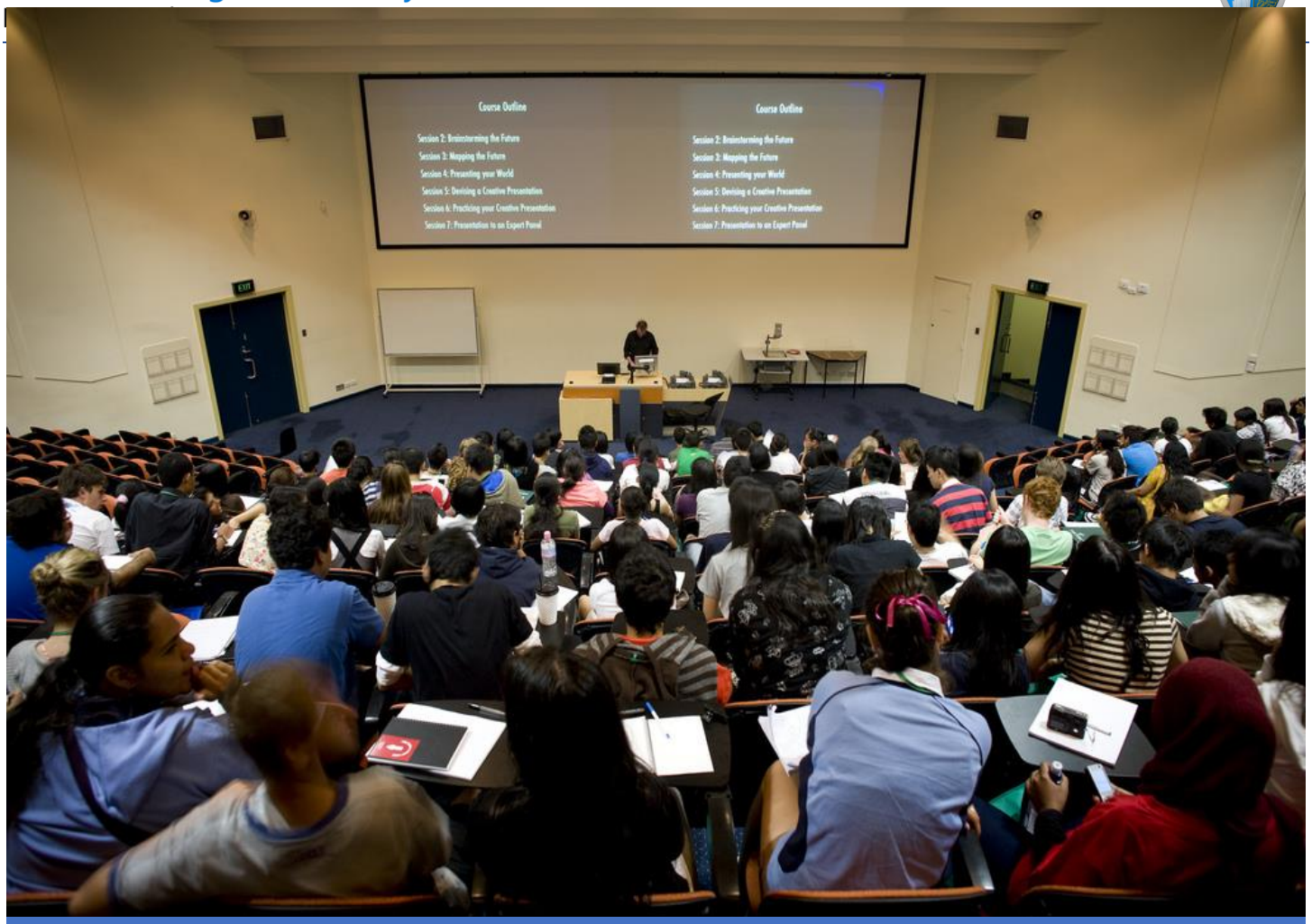
Why do this certification with Knights Innovation Support Centre.

Our trainers all have industry experience for decades and have specific experience with implementing the Office 365 security & compliance environments for large clients over the last few years.

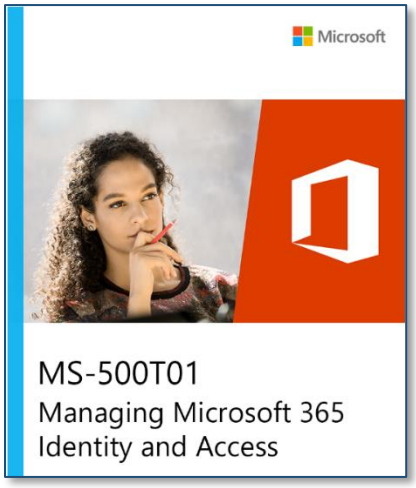
Doing this course with us includes access to the online practice tests that increases your chances of passing the international exams on your first attempt.

We have an excellent reputation for delivering excellence when it comes to the overall experience of our delegates – especially for our technical programs where it is important that the instructor is a Microsoft Certified Trainer for more than a decade with industry experience for several decades. The students who have attended our programs have always been happy with the overall experience and especially happy with the industry insights given by an experienced architect.

For more information on joining one of the programs please contact Séan Achim on 084 061-5472 or drop him an email on sean@Knights-ISC.co.za.



Course Outlines & Details



Managing Microsoft 365 Identity and Access

About this course

Help protect against credential compromise with identity and access management. In this course you will learn how to secure user access to your organization's resources. Specifically, this 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. You will also learn about solutions for managing external access to your Microsoft 365 system.

Audience profile

This course is for the Microsoft 365 security administrator role. This role collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and 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 has strong skills and experience with identity protection, information protection, threat protection, security management and data governance. This role focuses on the Microsoft 365 environment and includes hybrid environments.

At course completion

After completing this course, students should be able to:

- Administer user and group security in Microsoft 365.
- Manage passwords in Microsoft 365.
- Describe Azure Identity Protection features.
- Plan and implement Azure AD Connect.
- Manage synchronized identities.
- Plan and implement federated identities.
- Describe and use conditional access.

Course Outline

Module 1: User and Group Security

This module explains how to manage user accounts and groups in Microsoft 365. It introduces you to Privileged Identity Management in Azure AD as well as Identity Protection. **The module sets the foundation for the remainder of the course.**

Lessons

- Introduction to Identity and Access Management
- User Accounts in Microsoft 365
- Administrator Roles and Security Groups in Microsoft 365
- Password Management in Microsoft 365
- Azure AD Identity Protection

After completing this module, students should be able to:

- Describe the user identities in Microsoft 365.
- Create and manage user accounts.
- Describe and use Microsoft 365 admin roles.
- Describe the various types of group available in Microsoft 365.
- Plan for password policies and authentication.
- Implement Multi-factor authentication in Office 365.
- Describe Azure Identity Protection and what kind of identities can be protected.
- Enable Azure Identity Protection.
- Identify vulnerabilities and risk events.

Module 2: Identity Synchronization

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

Lessons

- Introduction to Identity Synchronization
- Planning for Azure AD Connect
- Implementing Azure AD Connect
- Managing Synchronized Identities
- Introduction to Federated Identities

After completing this module, students should be able to:

- Describe the Microsoft 365 authentication options.
- Explain directory synchronization.
- Plan directory synchronization.
- Describe and use Azure AD Connect.
- Configure Azure AD Connect Prerequisites.
- Manage users with directory synchronization.
- Manage groups with directory synchronization.
- Use Azure AD Connect Sync Security Groups.
- Describe claims-based authentication and federation trusts.
- Describe how AD FS works.

Module 3: Access Management

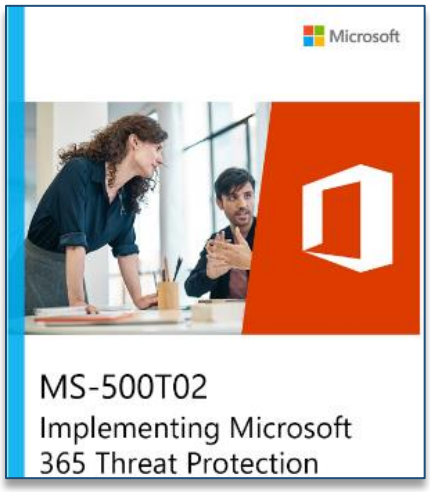
This module describes Conditional Access for Microsoft 365 and how it can be used to control access to resources in your organization. The module also explains Role Based Access Control (RBAC) and solutions for external access.

Lessons

- Conditional Access
- Managing Device Access
- Role Based Access Control (RBAC)
- Solutions for External Access

After completing this module, students should be able to:

- Describe the concept of conditional access.
- Describe conditional access policies.
- Plan for device compliance.
- Configure conditional users and groups.
- Configure RBAC.
- Distinguish between Azure RBAC and Azure AD administrative roles.
- Manage External Access.
- Explain Licensing Guidance for Azure AD B2B Collaboration.



Implementing Microsoft 365 Threat Protection

About this course

Threat protection helps stop damaging attacks with integrated and automated security. In this course 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 for them.

You will learn about Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and threat management. It also discusses securing mobile devices and applications. The goal of this course is to help you configure your Microsoft 365 deployment to achieve your desired security posture.

Audience profile

This course is for the Microsoft 365 security administrator role. This role collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and 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 has strong skills and experience with identity protection, information protection, threat protection, security management and data governance. This role focuses on the Microsoft 365 environment and includes hybrid environments.

At course completion

After completing this course, students will be able to:

- Describe cyber-attack threat vectors.
- Describe security solutions for Microsoft 365
- Use Microsoft Secure Score to evaluate your security posture.
- Use the Security Dashboard in the Microsoft Security & Compliance center.
- Configure various advanced threat protection services for Microsoft 365.
- Configure Advanced Threat Analytics.
- Plan and deploy secure mobile devices.

Course Outline

Module 1: Security in Microsoft 365

This module starts by explaining the various cyber-attack threats that exist. It then introduces you to the Microsoft solutions to thwart 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
- Security Solutions for Microsoft 365
- Microsoft Secure Score

On completion, students will be able to:

- Describe several techniques hackers use to compromise user accounts through email.
- Describe techniques hackers use to gain control over resources.
- List the types of threats that can be avoided by using Exhange Online Protection and Office 365 ATP.
- Describe the benefits of Secure Score and what kind of services can be analyzed.
- Describe how to use the tool to identify gaps between your current state and where you would like to be with regards to security.

Module 2: Advanced Threat Protection

This module explains the various threat protection technologies and services available in Microsoft 365. Specifically, the module covers message protection through Exchange Online Protection, Azure Advanced Threat Protection and Windows Defender Advanced Threat Protection.

Lessons

- Exchange Online Protection
- Office 365 Advanced Threat Protection
- Managing Safe Attachments
- Managing Safe Links
- Azure Advanced Threat Protection
- Microsoft Defender Advanced Threat Protection

On completion, students 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 to malicious websites.
- Configure Azure Advanced Threat Protection.
- Configure Windows Defender ATP.
- Integrate Windows Defender ATP with Azure ATP.

Module 3: Threat Management

This module explains Microsoft Threat Management which provides you with the tools to evaluate and address cyber threats. You will learn how to use the Security Dashboard in the Microsoft 365 Security and Compliance Center. It also explains and configures Microsoft Advanced Threat Analytics.

Lessons

- Microsoft 365 Threat Intelligence
- Using the Security Dashboard
- Configuring Advanced Threat Analytics

On completion, students will be able to:

- Describe how threat intelligence in Microsoft 365 is powered by the Microsoft Intelligent Security Graph.
- 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, global trends, protection quality, and the organization's exposure to threats.
- Describe how the Security dashboard can be used as a launching point to enable security analysts to drill down for more details by using Threat Explorer.
- 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.

Module 4: Mobility

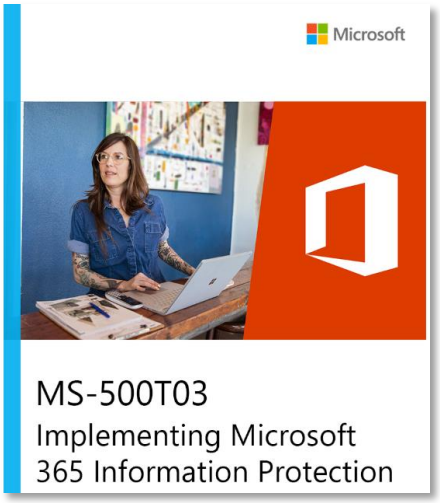
This module is all about securing mobile devices and applications. You will learn about Mobile Device Management and how it works with Intune. You will also learn about how Intune and Azure AD can be used to secure mobile applications.

Lessons

- Plan for Mobile Application Management
- Plan for Mobile Device Management
- Deploy Mobile Device Management
- Enroll Devices to Mobile Device Management

On completion, students will be able to:

- Describe mobile application considerations.
- Use Intune to manage mobile applications.
- Manage devices with MDM.
- Compare MDM for Office 365 and Intune.
- Configure Domains for MDM.
- Manage Device Security Policies.
- Define Corporate Device Enrollment Policy.
- Enroll devices to MDM.



Implementing Microsoft 365 Information Protection

About this course

Information protection is the concept of locating and classifying data anywhere it lives. In this course you will learn about information protection technologies that help secure your Microsoft 365 environment. Specifically, this course discusses information rights managed content, message encryption, as well as labels, policies and rules that support data loss prevention and information protection. The course also explains deployment of Microsoft Cloud App Security.

Audience profile

This course is for the Microsoft 365 security administrator role. This role collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and 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 has strong skills and experience with identity protection, information protection, threat protection, security management and data governance. This role focuses on the Microsoft 365 environment and includes hybrid environments.

At course completion

After completing this course, learners should be able to:

- Implement information rights management.
- Secure messages in Office 365.
- Configure Data Loss Prevention policies.
- Deploy and manage Cloud App Security.
- Implement Azure information protection for Microsoft 365.
- Implement Windows information protection for devices.

Course Outline

Module 1: Information Protection

The module introduces how to implement Azure Information Protection and Windows Information Protection.

Lessons

- Information Rights Management
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption
- Azure Information Protection
- Advanced Information Protection
- Windows Information Protection

On completion, students will be able to:

- Configure labels and policies for Azure Information Protection.
- Configure the advance AIP service settings for Rights Management Services (RMS) templates.
- Plan a deployment of Windows Information Protection policies.

Module 2: Rights Management and Encryption

This module explains information rights management in Exchange and SharePoint. It also describes encryption technologies used to secure messages.

Lessons

- Information Rights Management
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption

On completion, students will be able to:

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

Module 3: Data Loss Prevention

This module is all about data loss prevention in Microsoft 365. You will learn about how to create policies, edit rules, and customize user notifications.

Lessons

- Data Loss Prevention Explained
- Data Loss Prevention Policies
- Custom DLP Policies
- Creating a DLP Policy to Protect Documents
- Policy Tips

On completion, students will be able to:

- Describe Data Loss Prevention (DLP).
- Recognize how actions and conditions work together for DLP.
- Use policy templates to implement DLP policies for commonly used information.
- Describe the different built-in templates for a DLP policies.
- 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.
- Describe how to work with managed properties for DLP policies.
- Explain how SharePoint Online creates crawled properties from documents.
- Describe the user experience when a user creates an email that contains sensitive information.

Module 4: Cloud Application Security

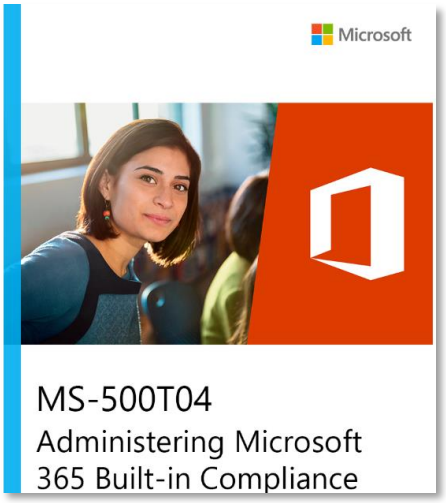
This module is all about cloud app security for Microsoft 365. The module will explain cloud discovery, app connectors, policies, and alerts.

Lessons

- Cloud Application Security Explained
- Using Cloud Application Security Information

On completion, students will be able to:

- Describe Cloud App Security.
- Explain how to deploy Cloud App Security.
- Control your Cloud Apps with Policies.
- Troubleshoot Cloud App Security.
- Use the Cloud App Catalog.
- Use the Cloud Discovery Dashboard.
- Prepare for Office 365 Cloud App Security.
- Manage cloud app permissions.



Administering Microsoft 365 Built-in Compliance

About this course

Internal policies and external requirements for data retention and investigation may be necessary for your organization. In this course you will learn about archiving and retention in Microsoft 365 as well as data governance and how to conduct content searches and investigations.

Specifically, 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. The course also helps your organization prepare for Global Data Protection Regulation (GDPR).

Audience profile

This course is for the Microsoft 365 security administrator role. This role collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and 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 has strong skills and experience with identity protection, information protection, threat protection, security management and data governance. This role focuses on the Microsoft 365 environment and includes hybrid environments.

At course completion

After completing this course, learners should be able to:

- Plan and deploy a data archiving and retention system.
- Perform assessments in Compliance Manager.
- Manage email retention through Exchange.
- Conduct an audit log investigation.
- Create and manage an eDiscovery investigation.
- Manage GDPR data subject requests

Course Outline

Module 1: Archiving and Retention

This module explains concepts related to retention and archiving of data for Microsoft 365 including Exchange and SharePoint.

Lessons

- Archiving in Microsoft 365
- Retention in Microsoft 365
- Retention Policies in the Compliance Center
- Archiving and Retention in Exchange
- In-place Records Management in SharePoint

On completion, students will be able to:

- Describe 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 the Microsoft Compliance center.
- Explain how a retention policy works.
- Create a retention policy.
- Enable and disable In-Place Archiving.
- Create useful retention tags.

Module 2: Data Governance in Microsoft 365

This module focuses on data governance in Microsoft 365. The module will introduce you to Compliance Manager and discuss GDPR.

Lessons

- Planning Compliance Needs
- Building ethical walls in Exchange Online
- Manage Retention in Email
- Troubleshooting Data Governance

On completion, students will be able to:

- Plan security and compliance roles.
- Describe what you need to consider for GDPR.
- Describe what an ethical wall in Exchange is and how it works.
- Work with retention tags in mailboxes
- Describe retention policies with email messages and email folders
- Explain how the retention age of elements is calculated.
- Repair retention policies that do not run as expected.

Module 3: Managing Search and Investigations

This module is focused on content searching and investigations. Specifically, it covers how to use eDiscovery to conduct advanced investigations of Microsoft 365 data. It also covers audit logs and discusses GDPR data subject requests.

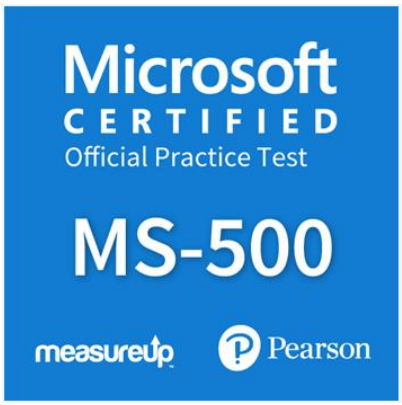
Lessons

- Content Search
- Audit Log Investigations
- Advanced eDiscovery

On completion, students will be able to:

- Describe how to use content search.
- Designing your content search.
- Configuring search permission filtering.
- Describe what the audit log is and the permissions that are necessary to search the Office 365 audit log.
- Configure Audit Policies.
- Enter criteria for searching the audit log.
- Export search results to a CSV file.
- Describe what Advanced eDiscovery is and what requirements are needed.
- Analyze data in Advanced eDiscovery.
- Viewing the Advanced eDiscovery event log.
- Use Express Analytics.

On-Line Practice Test (60 Days Access)



About the online Microsoft Official Practice Test powered by MeasureUp

The MeasureUp MS-500: Microsoft 365 Security Administration practice test is designed to help candidates prepare for and pass the Microsoft MS-500 exam.

The exam is aimed at Administrators who want to test their knowledge implementing and managing identity and access, implementing and managing threat protection, implementing and managing information protection and managing governance and compliance features in Microsoft 365.

This exam counts as credit toward the following certifications:

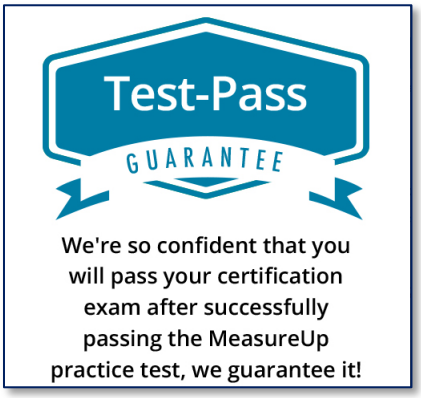
Microsoft 365 Certified: Security Administrator Associate

This test contains 121 questions and covers the following objectives:

- Implement and manage identity and access - 42
- Implement and manage threat protection - 27
- Implement and manage information protection - 22
- Manage governance and compliance features in Microsoft 365 - 30

Why Choose the Microsoft Official Practice?

Quality test content is extremely important to us so that you will be prepared on exam day. We ensure that all objectives of the exam are covered in depth so you'll be ready for any question on the exam. Our practice tests are written by industry experts in the subject matter. They work closely with certification providers to understand the exam objectives, participate in beta testing and take the exam themselves before creating new practice tests. Our quality content and innovative technology have earned the prestigious credential of Microsoft Certified Practice Test Provider.



- Online performance-based simulations give hands on work environment experience
- Questions are similar to exam questions so you test your knowledge of exam objectives
- Detailed explanations for both correct and distractor answers reinforce the material
- Study Mode covers all objectives ensuring topics are covered
- Certification Mode (timed) prepares students for exam taking conditions
- Instant, drill-down score reports tell you exactly the areas to focus on.

Option Details

- Microsoft Official Practice Test
- Detailed answers and references
- Study and timed certification mode
- Instant score report
- Cost: $110