MICROSOFT

Microsoft 365 Certified: Security Administrator Associate

Validate your technical skills and grow your career.

This certification demonstrates that the recipient is proficient in neutralizing threats by securing the Office 365 environment, implementing security complains solutions and enforcing data policies.

Why Take The Microsoft 365 Certified: Security Administrator MS-700 Exam?

Show your organization that you can effectively secure the cloud-based Microsoft 365 suite by utilizing cybersecurity defense solutions.

Increase My Salary:

- The average salary for someone who holds a Microsoft Certified: Security Administrator Associate certification is around $105,000 / year.

Be Part Of The Team:

- Be the first line of defense for your organization and team to any security threats that may arise.

Abilities Validated By The Certification:

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

Recommended Knowledge & Experience:

- While it's not required, it is recommended that the candidate already has their Microsoft 365 Fundamentals Certification before taking the exam.

Exam Topics & Scoring:

Exam MS-500: Microsoft 365 Security Administration

IMPLEMENT AND MANAGE IDENTITY AND ACCESS (30-35%)

Secure Microsoft 365 hybrid environments

- plan Azure AD authentication options
- plan Azure AD synchronization options
- monitor and troubleshoot Azure AD Connect events

Secure Identities

- implement Azure AD group membership
- implement password management
- configure and manage identity governance

Implement authentication methods

- plan sign-on security ⬜ implement multi-factor authentication (MFA)
- manage and monitor MFA
- plan and implement device authentication methods like Windows Hello
- configure and manage Azure AD user authentication options

Implement conditional access

- plan for compliance and conditional access policies
- configure and manage device compliance for endpoint security
- implement and manage conditional access

Implement role-based access control (RBAC)

- plan for roles
- configure roles
- audit roles Implement Azure AD Privileged Identity Management (PIM)
- plan for Azure PIM
- implement and configure Azure PIM roles

- manage Azure PIM role assignments

Implement Azure AD Identity Protection

- implement user risk policy
- implement sign-in risk policy
- configure Identity Protection alerts
- review and respond to risk events

IMPLEMENT AND MANAGE THREAT PROTECTION (20-25%)

Implement an enterprise hybrid threat protection solution

- plan an Azure ATP solution
- install and configure Azure ATP
- monitor and manage Azure ATP

Implement device threat protection

- plan a Microsoft Defender ATP solution
- implement Microsoft Defender ATP
- manage and monitor

Microsoft Defender ATP Implement and manage device and application protection

- plan for device and application protection
- configure and manage Windows Defender Application Guard
- configure and manage Windows Defender Application Control
- configure and manage Windows Defender Exploit Guard
- configure Secure Boot
- configure and manage Windows device encryption
- configure and manage non-Windows device encryption
- plan for securing applications data on devices
- implement application protection policies

Implement and manage Office 365 ATP

- configure Office 365 ATP
- monitor Office 365 ATP
- conduct simulated attacks using Attack Simulator

Implement Azure Sentinel for Microsoft 365

- plan and implement Azure Sentinel
- configure playbooks in Azure Sentinel
- manage and monitor Azure Sentinel
- respond to threats in Azure Sentinel

IMPLEMENT AND MANAGE INFORMATION PROTECTION (15-20%)

Secure data access within Office 365

- implement and manage Customer Lockbox
- configure data access in Office 365 collaboration workloads
- configure B2B sharing for external users

Manage Azure information Protection (AIP)

- plan an AIP solution
- configure Sensitivity labels and policies
- deploy the RMS connector
- manage tenant keys
- deploy the AIP client
- integrate AIP with Office 365 Services

Manage Data Loss Prevention (DLP)

- plan a DLP solution
- create and manage DLP policies
- create and manage sensitive information types
- monitor DLP reports
- manage DLP notifications

Implement and manage Microsoft Cloud App Security

- plan Cloud App Security implementation
- configure Microsoft Cloud App Security
- manage cloud app discovery
- manage entries in the Cloud app catalog
- manage apps in Cloud App Security
- manage Microsoft Cloud App Security
- configure Cloud App Security connectors and Oauth apps
- configure Cloud App Security policies and templates
- review, interpret and respond to Cloud App Security alerts, reports, dashboards and logs

MANAGE GOVERNANCE AND COMPLIANCE FEATURES IN MICROSOFT 365 (25- 30%)

Configure and analyze security reporting

- monitor and manage device security status using Microsoft Endpoint Manager Admin Center
- manage and monitor security reports and dashboards using Microsoft 365 Security Center
- plan for custom security reporting with Graph Security API ⬜ use secure score dashboards to review actions and recommendations
- configure alert policies in the Security & Compliance admin center

Manage and analyze audit logs and reports

- plan for auditing and reporting
- perform audit log search
- review and interpret compliance reports and dashboards
- configure audit alert policy

Manage data governance and retention

- plan for data governance and retention
- review and interpret data governance reports and dashboards
- configure retention policies
- define data governance event types
- define data governance supervision policies
- configure Information holds
- find and recover deleted Office 365 data
- configure data archiving
- manage inactive mailboxes

Manage search and investigation

- plan for content search and eDiscovery
- search for personal data
- monitor for leaks of personal data
- delegate permissions to use search and discovery tools
- use search and investigation tools to perform content searches
- export content search results
- manage eDiscovery cases

Manage data privacy regulation compliance

- plan for regulatory compliance in Microsoft 365
- review and interpret GDPR dashboards and reports
- manage Data Subject Requests (DSRs)
- administer Compliance Manager
- review Compliance Manager reports
- create and perform Compliance Manager assessments and action items

Prepare for your exam:

The best way to prepare is with first-hand experience. Taking advantage of the opportunities that Phoenix TS provides will assist you with gathering all the knowledge and skills you'll need for certification.

Phoenix TS Microsoft 365 Certified: Security Administrator Associate – Learning Pathways

- ### **MS-500T00: Microsoft 365 Security Administration**

Course Overview Phoenix TS' 4-day instructor-led Microsoft 365 Security Administration training and certification boot camp in Washington, DC Metro, Tysons Corner, VA, Columbia, MD or Live Online you will learn how to secure user access to your organization's resources. The course covers user password protection, multi-factor authentication, how to enable Azure Identity Protection, how to […]

Click To Read More

1 –

https://www.globalknowledge.com/us-en/resources/resource-library/articles/top-paying-certifications/?utm_source=Sales-Enablement&utm_medium=White-Paper&utm_campaign=&utm_content=Top-Paying-Certs

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

Exam Details

- Multiple choice, multiple answers
- Testing in person or online proctored exam

- 130 Min to take the test
- $150 test fee
- Available in English, Japanese, Korean, and Simplified Chinese