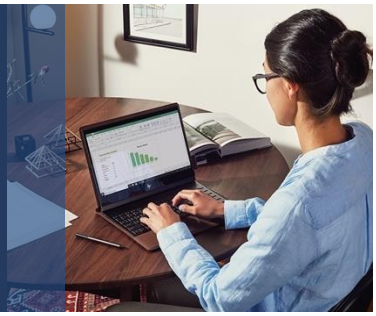
Microsoft

Microsoft Security, Compliance, and Identity Fundamentals

ASSESSMENT GUIDE



Overview

This document provides assessments for SC-900T00 Microsoft Security, Compliance, and Identity Fundamentals. The assessment consists of a set of items for each course module that can be used throughout the course to monitor student progress and inform your instruction; the assessment items are a mixture of multiple-choice questions and open-ended questions.

This guide is intended to be a reference and starting point for instructors as you plan how to assess your students. As you read through the guide, you may choose to tailor the assessment strategies, including the assessment items and rubric, for your classroom.

Table of Contents

Module Questions

Introduction

This section includes multiple choice and open-ended questions that are aligned to the course modules for SC900T00 Microsoft Security, Compliance, and Identity Fundamentals. Each module includes multiple-choice questions and open-ended questions.

You are free to use the questions as they are currently presented or modify as appropriate for your classes. The questions do not appear in any other course materials and are designed to supplement the formative assessment opportunities that are integrated directly into Microsoft Learn and the Microsoft Official Course (e.g., Knowledge Checks, "Try-It" activities, Exercises, Walkthroughs, Labs). They are also designed to allow for easy integration into an online quiz through Microsoft Forms or through your institution's Learning Management System (LMS). Each set of module questions represents indicative coverage for each module objective domain.

Assigning the module questions to students as an independent activity will enable you to collect data about individual student progress. However, we recommend that you set aside class time to review answers and address any common student misconceptions, as later modules depend on knowledge and understanding gained earlier in the course.

Overview of multiple-choice questions

The multiple-choice questions require one or more answer responses and will include plausible distractors. These are set at a level slightly lower than the multiple-choice questions in the Exam SC-900: Microsoft Security, Compliance, and Identity Fundamentals

Overview of open-ended questions

The open-ended questions present further challenges beyond single answer responses and include scenario-based questions. These questions give students the opportunity to demonstrate critical thinking through their responses.

Module 1: Describe the concepts of security, compliance, and identity

Multiple choice questions

1. Which of the following are principles of the Zero Trust model?

   Select all that apply.

   a. Verify explicitly (correct answer)

   b. Block access

   c. Least privileged access (correct answer)

   d. Assume breach (correct answer)

2. The shared responsibility model, identifies which security tasks are handled by the cloud provider, and which security tasks are handled by you, the customer. The responsibilities vary depending on where the workload is hosted. Which approach places more of the responsibility on the cloud provider?

   Select the correct option.

   a. On-premises datacenter

   b. Infrastructure as a Services (IaaS)

   c. Software as a Service (SaaS) (correct answer)

   d. Platform as a Service (PaaS)

3. Consider the shared responsibility model, in which approach does the customer own the security tasks related with information & data, devices, and accounts & identities?

   Select the correct option.

   a. On-premises datacenter

   b. Infrastructure as a Services (IaaS) AND Platform as a Service (PaaS)

   c. Software as a Service (SaaS) (correct answer)

   d. All the above (correct answer)

4. The HTTPS protocol is an example of which type of encryption?

   Select the correct option.

   a. Encryption in transit

   b. Encryption at rest

c. No encryption

d. Hashing

5. What is the term used to describe the process for verifying the identity of an object, service, or person?

Select the correct option.

a. Authorization

b. Authentication (correct answer)

c. Auditing

d. Administration

Open-ended questions

1. A client wants to implement a Zero Trust security strategy that is based on the three key principles: verify explicitly, least privilege access, and assume breach. As they consider their strategy, what elements/pillars should they account for to provide an end-to-end Zero Trust security strategy and what are examples of the types of security considerations they should consider for each element/pillar?

Answer: (Should include the six pillars: identities, devices, applications, data, infrastructure, and networks. Refer to the content to see explicit examples for each. This topic will be revisited in subsequent modules as you further explore identity, security, and compliance.)

2. The shared responsibility identifies which security tasks are handled by the cloud provider, and which security tasks are handled by you, the customer. The responsibilities vary depending on where the workload is hosted. For each approach to hosting (On-premises datacenter, IaaS, PaaS, and SaaS) describe the types of security responsibilities that would be owned by the customer vs. those the cloud provider.

Answer: (The responses should reflect that as the customer moves from On-Prem to IaaS to PaaS to SaaS, more of the responsibility shifts to the cloud provider. Also, and very importantly, the answer should reflect that fact that regardless of which hosting is used, the customer always owns information and data, devices, and accounts & identities.)

3. Defense in depth uses a layered approach to security, rather than relying on a single perimeter. What are examples of security layers and what are examples of security measures that can be taken for each layer described?

Answer: (Should include the 7 layers included the training content: physical security, identity & access, perimeter, network, compute, application, and data. Refer to the training content for some examples the types of security measures that can be applied to each.)

4. The CIA, triangle is a way to think about security trade-offs. Identify what each letter stands for and describe what each letter refers to.

Answer: (Should include the terms Confidentiality, Integrity, and Availability. Refer to the training content for description of what is referred to by each of these three components.)

5. Identity has become the new security perimeter. Describe what is meant by this and the drivers that have led to a shift from a traditional perimeter-based security model to identity as the new security perimeter?

Answer: (Should include a statement about what is an identity and drivers that have led to this concept, including the acceleration in number of people working from home, SaaS applications that are hosted outside of the corporate network, the use of personal devices to access corporate resources, the use of unmanaged devices by partners and customers who may need to access your corporate resources, proliferation of IoT devices, and more.)

Module 2: Describe the capabilities of Microsoft Identity and access management solutions

Multiple choice questions

1. What are the external identity types supported by Azure AD?

   Select all that apply.

   a. B2B (correct answer)

   b. B2C (correct answer)

   c. Device identity

   d. Application identity

2. Which of the following verification methods can be used with Azure Active Directory multifactor authentication?

   Select all that apply.

   a. Microsoft Authenticator app (correct answer)

   b. SMS (correct answer)

   c. Voice call (correct answer)

   d. Security questions

3. Self-service password reset (SSPR) works in the following scenarios?

   Select all that apply.

   a. Password change (correct, but there is a better answer)

   b. Password reset (correct, but there is a better answer)

   c. Account unlock (correct, but there is a better answer)

   d. All the above (correct answer)

4. Which of the following are signals that can be used by conditional access?

   Select all that apply.

   a. Named location information (correct, but there is a better answer)

   b. User risk (correct but there is a better answer)

c. User or group membership (correct but there is a better answer)

d. All the above (correct answer)

5. How does Privileged Identity Management (PIM) mitigate the risks of excessive, unnecessary, or misused access permissions to Azure resources and Azure AD

Select all that apply.

a. time-based role activation (correct answer)

b. approval based role activation (correct answer)

c. password-based role activation

d. risk-based role activation

Open-ended questions

1. Describe the different identity types supported by Azure AD and when you would use each.

Answer: (Should include the following identity types: user, service principal, managed identity, and device. When describing the user identity type, the response should include the different external identities supported by Azure AD (B2B and B2C). When referring to Service Principal, the response should reference the point that a service principal is like an identity for an application. Reference to a managed identity should include reference to system-assigned and user assigned and some of the differences. Lastly, the reference to a device identity types should reference the multiple options for getting devices into Azure AD.)

2. You friends just started a small business and are using a free tier of Azure AD. They want to increase security but are not sure where to start and are on a very limited budget. They know that you just received your Microsoft Security, Compliance, and Identity Fundamentals certification, so they reach out to you for some guidance. What would you suggest and why?

Answer: (Should include a statement about security defaults in Azure AD, some of the features of security defaults including enforcing multifactor authentication registration for all users. Additionally, the answer should include that security defaults is available with the free tier of Azure AD.)

3. Your customer is looking to implement an extra layer of security before allowing authenticated users to access data or other assets. They want to have the ability to manage and control access to resources based on different conditions/signals. Which Azure AD feature would you recommend and how would you describe how that feature works and its benefits?

Answer: (Should describe Conditional Access in Azure AD and include a statement about how signals are used to make decisions, the analogy to if/then statements may be included. Additionally, the answer should include reference to the different types of signals and the types of decisions that can be made based on those signals. Lastly, the answer should include reference to the fact that conditional access is implemented through policies that are created in Azure AD. Bonus points if they tie the benefits back to Zero Trust methodology)

4. Your customer is facing challenges in managing both employee and business partner access to corporate resources, at scale. There have been issues with people having access much longer than they need it. They already have Azure AD Premium P2, so which features of Azure AD would you recommend and why?

Answer: (Should include a statement that references entitlement management and its benefits, including the ability to manage access for internal and external users, the ability to create access packages, and access reviews. Refer to the training content for details.)

5. Your customer is looking for a solution to detect and remediate identity related risks. They already have Azure AD Premium P2, what solution would you offer and why? Also describe the capabilities the solutions offer.

Answer: (Should include a statement that references Azure Identity Protection and describe the tasks: the ability to automate and remediate identity-based risks, investigate risks, and export risk detection data to 3rd party utilities for analysis. Also describe the types of risks (sign-in and user risk, that can be detected and the type of reports the solution can provide. Refer to the training content for more details.)

Module 3: Describe the capabilities of Microsoft security solutions

Multiple choice questions

1. An attacker can bring down your website by sending a large volume of network traffic to your servers. Which Azure service can help protect from this kind of attack?

Select the correct option.

a. Azure Firewall

b. Azure DDoS protection **(correct answer)**

c. Network security groups (NSGs)

d. Bastion

2. Which capability in Azure security center provides the ability to look at the topology of your workloads, so you can see if each node is properly configured.

Select the correct option.

a. Secure Score

b. Azure Policy

c. Network map (correct answer)

d. Resource health score

3. Which Azure security solution provides different plans that can be enabled separately and will run simultaneously to provide a comprehensive defense for compute, data, and service layers in your environment?

Select the correct option.

a. Azure Defender (correct answer)

b. Azure Sentinel

c. Azure Security Baselines

d. Azure Policy

4. Which capability of Azure Sentinel can help automate and orchestrate your response to incidents and common security tasks?

Select the correct option.

a. Workbooks

b. Security playbooks (correct answer)

c. Connectors

d. the MITRE framework

5. Employees in your organization want to use their personal devices for work but they do not want their phones to be under full corporate control. Which capability allows admin to protect corporate data at the application level?

Select the correct option.

a. Mobile device management

b. Mobile application Management (correct answer)

c. Role based access control

d. Intune security baseline

Open-ended questions

1. Describe how and enterprise would use both Azure Firewall and Azure Network Security groups to protect resources in your virtual networks?

Enter your answer in the following space.

Answer: (Should include statement about how NSGs and Azure Firewall each work to protect resources in your virtual network. NSGs allow/deny traffic to/from Azure sources in the vnet, based on rules. Azure Firewall also protects your Azure virtual network, but the best approach is to use Azure Firewall on a centralized virtual network. Azure Firewall complements NSG functionality. Together they provide better defense-in-depth network security. Network security groups provide distributed network layer traffic filtering to limit traffic to resources within virtual networks in each subscription. Azure Firewall is a fully stateful, centralized network firewall as-a-service, which provides network- and application-level protection across different subscriptions and virtual networks. Refer to https://docs.microsoft.com/en-us/azure/firewall/firewall-faq#what-is-the-difference-between-network-security-groups--nsgs--and-azure-firewall)

2. You have a meeting with your customer to talk about Microsoft Defender, an enterprise-wide defense suite, with the ability to detect, prevent, investigate, and respond to. Describe, as you would to the customer, each of the component solutions, what areas of protection they address, and how they address security needs.

Enter your answer in the following space.

Answer: (Should include a statement that mentions the 4 solution areas of Microsoft Defender: Microsoft Defender for Identity, Defender for Endpoint, MCAS, and Defender for Office 365. Refer

to the training content for details on each. Bonus points for those who can tie the benefits back to the Zero Trust methodology.)

3. What are the capabilities of the cloud app security framework upon which the Microsoft Cloud App security (MCAS) is built?

Enter your answer in the following space.

Answer: (Should include a statement that mentions: a) discover and control the use of Shadow IT, b) protect your sensitive information anywhere in the cloud, c) protect against cyberthreats and anomalies, and d) assess your cloud apps' compliance. Provide brief explanation of each. Refer to the training content.)

4. Your organization uses Azure services and Microsoft 365. The IT organization needs to understand their current security posture and how to improve it. What solutions can provide this capability? Describe how the solutions can help improve their security posture.

Enter your answer in the following space.

Answer: (Should include a statement about Azure Security Center, how Security center provides a continuous assessment of the entire estate with recommendations, the network map, and Secure score. Since the customer has both Azure services and Microsoft 365, the answer also needs to include reference to Microsoft Secure score which is found in the Microsoft 365 Defender portal and the information that is provided in the improvement actions tab, which is analogous to the recommendations that are part of provided by Azure continuous assessment in Azure security center. The learner should also be able to articulate the difference between Azure secure score and Microsoft Secure score, although they are similar, they measure different things. Azure Security Center is a measure of the security posture of your Azure subscriptions. Secure Score in the Microsoft 365 Defender portal is a measure of the security posture of the organization across your apps, devices, and identities.)

5. Describe the different ways admins can manage endpoint security with Intune.?

Enter your answer in the following space.

Answer: (Should include a statement that includes using endpoint security policies, using device compliance policies, integrating with Azure AD to configure conditional access. and integration with Microsoft Defender for Endpoint.)

Module 4: Describe the capabilities of Microsoft compliance solutions

Multiple choice questions

1. Aside from the global administrator role, which roles can provide access to the to the Microsoft 365 Compliance center?

Select all that apply.

a. Compliance administrator (correct answer)

b. Compliance data administrator (correct answer)

c. User administrator

d. Neither Ingress nor Egress

2. What do sensitive information types use to classify data?

Select all that apply.

a. Artificial intelligence and machine learning (correct answer).

b. Patterns defined by a regular expression (regex) or a function (correct answer).

c. String length

d. All the above.

3. Advanced audit supports the long-term retention of audit log for up to _____ years.

Select all that apply.

a. 5 years

b. 3 years

c. 10 years (correct answer)

d. 25 years

4. Which Azure capability enables development teams to rapidly provision and run new environments, with the knowledge that they're in line with the organization's compliance requirements.

Select the correct option.

a. ARM templates

b. Azure policies

c. Azure Blueprints (correct answer)

d. Azure baselines

5. If you want to prevent accidental deletion of an Azure resource, which of the following options should you use?

Select the correct option.

a. MFA

b. Azure tags

c. Azure resource locks (correct answer)

d. Azure policies

Open-ended questions

1. Compliance score measures progress in completing recommended improvement actions within controls. Describe the different actions that are part of compliance score and how they are categorized.

Answer: (Should include a statement that mentions the two types of actions: actions that the organization is expected to manage and actions that Microsoft manages for the organization. Additionally, the response should include the types of categories: mandatory and discretionary, preventive, detective, and corrective.)

2. Describe the ways in which sensitivity labels provide information protection?

Answer: (Should include a how sensitivity labels can be used to encrypt email and documents, mark the content with watermarks, headers, or footers, apply the label automatically or prompt users to apply the label, protect content in containers such as sites and groups (by controlling access to the container), extending sensitivity labels to third-party apps and services, and classifying content that persists with the content?)

3. Your organization is looking to implement solutions to mitigate risk from within the organization (insider risk solutions). What are some of the different solutions that can be offered and how they do address insider risk?

Answer: (Should include a statement that mentions one or more of the following and how they address insider risk:

- **insider risk management – helps minimize internal risks by enabling an organization to detect, investigate, and act on risky and malicious activities – refer to the workflow.**
- **communication compliance - helps minimize communication risks by enabling organizations to detect, capture, and take remediation actions for inappropriate messages.**
- **information barriers - policies that admins can configure to prevent individuals or groups from communicating with each other.**
- **privileged access management - allows granular access control over privileged admin tasks; and**

- **Customer Lockbox ensures that Microsoft can't access the content to perform a service operation without explicit approval.)**

4. Describe the purpose of eDiscovery?

Answer: (Should include a statement that Sometimes a company may become involved in litigation and need to find electronic information to be used as evidence. Electronic discovery or eDiscovery tools, can be used to search for content in Exchange Online mailboxes, Microsoft 365 Groups, Microsoft Teams, SharePoint Online and OneDrive for Business sites, Skype for Business conversations, and Yammer teams.)

5. Describe the difference between Azure Policy and Azure role-based access control (RBAC)

Enter your answer in the following space.

Answer: (Should include statement that Azure Policy is used to ensure that the resource state is compliant to your organization's business rules, no matter who made the change or who has permission to make changes. Azure RBAC manages who has access to Azure resources, what they can do with those resources, and what areas they can access. If actions need to be controlled, then you would use Azure RBAC. If an individual has access to complete an action, but the result is a non-compliant resource, Azure Policy still blocks the action.**)**