Microsoft Security, Compliance, and Identity Fundamentals (SC-900) Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Don't worry about getting everything right, your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations, and take breaks to retain information better.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning.

7. Use Other Tools

Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly — adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. Which pillar of identity focuses on tracking resources accessed by users?

A. Authorization

B. Auditing

C. Administration

D. Authentication

2. With Advanced Audit in Microsoft 365, can you identify when email items were accessed?

A. Yes

B. No

C. Depends on the audit logs

D. Only for calendar items

3. Does enabling multi-factor authentication (MFA) increase the Microsoft Secure Score?

A. Yes

B. No

C. Only for administrators

D. Only for end users

4. What feature helps in monitoring Azure resources for abnormal activity and potential threats?

A. Azure Advisor

B. Azure Security Center

C. Azure Policy

D. Azure Backup Center

5. Which security feature is available in the free mode of Microsoft Defender for Cloud?

A. Threat protection alerts

B. Just-in-time (JIT) VM access to Azure virtual machines

C. Vulnerability scanning of virtual machines

D. Secure score

6. What are customers responsible for when evaluating security in a software as a service (SaaS) cloud services model?

A. operating systems

B. network controls

C. applications

D. accounts and identities

7. Which tasks can be performed by Azure Active Directory (Azure AD) Identity Protection? Select all that apply.

A. Configure external access for partner organizations

B. Export risk detection to third-party utilities

C. Automate the detection and remediation of identity based-risks

D. Investigate risks that relate to user authentication

8. Can Azure Active Directory (Azure AD) Identity Protection add users to groups based on the users' risk level?

A. Yes

B. No

C. Only for privileged users

D. Only for external users

9. What action is required to create cases in the Case dashboard?

A. Triage

B. Investigate

C. Action

D. Review

10. Which privacy principle of Microsoft ensures that individuals have control over their personal information?

A. Transparency

B. Control

C. Security

D. Integrity

Answers

1. B
2. A
3. A
4. B
5. D
6. D
7. C
8. B
9. B
10. B

Explanations

1. Which pillar of identity focuses on tracking resources accessed by users?

A. Authorization

B. Auditing

C. Administration

D. Authentication

The pillar of identity that focuses on tracking resources accessed by users is Auditing. This pillar involves the continuous monitoring and logging of user activities to ensure compliance and security within an organization. By implementing auditing practices, organizations can create a detailed record of who accessed what resources and when, allowing them to analyze patterns, detect anomalies, and respond to potential security threats. Auditing is crucial for maintaining accountability and ensuring that users only access data and resources they are authorized to use. It also supports compliance with various regulatory requirements by providing evidence of proper usage and any potential breaches. In contrast, while Authorization deals with granting or denying access rights based on a user's identity and role, and Administration refers to the management and configuration of identity and access policies, these aspects do not inherently involve tracking access activities like auditing does. Authentication, on the other hand, is the process of verifying a user's credentials before granting access to systems or resources, which is separate from the ongoing tracking of access behaviors.

2. With Advanced Audit in Microsoft 365, can you identify when email items were accessed?

A. Yes

B. No

C. Depends on the audit logs

D. Only for calendar items

Advanced Audit in Microsoft 365 provides enhanced visibility into how data is accessed and utilized within the environment. One of the significant capabilities of Advanced Audit is the ability to track various activities, including access to email items. With this feature, administrators can review detailed logs that indicate when specific email items were accessed. This tracking is crucial for organizations to ensure compliance, investigate potential security incidents, and monitor user activities. The data collected can help in audits and provide insights into user behavior, making it an invaluable tool for maintaining security protocols. This capability extends to not only emails but includes a range of other activities in the Microsoft 365 environment, allowing organizations to maintain a comprehensive understanding of data access and modifications.

3. Does enabling multi-factor authentication (MFA) increase the Microsoft Secure Score?

A. Yes

B. No

C. Only for administrators

D. Only for end users

Enabling multi-factor authentication (MFA) does indeed increase the Microsoft Secure Score. Microsoft Secure Score is a measurement of an organization's security posture, and implementing MFA is recognized as a critical step in enhancing security. MFA adds an additional layer of protection by requiring users to present multiple forms of identification before they can gain access to their accounts. This significantly reduces the risk of unauthorized access due to compromised passwords. As organizations implement increases in their security measures, such as MFA, their Secure Score reflects this improved security posture by increasing the overall score. This is because MFA is one of the recommended actions that Microsoft suggests for organizations to bolster their defenses against security threats. The inclusion of this feature not only enhances individual account security but also benefits the organization's overall security strategy, leading to a higher Secure Score as a result.

4. What feature helps in monitoring Azure resources for abnormal activity and potential threats?

A. Azure Advisor

B. Azure Security Center

C. Azure Policy

D. Azure Backup Center

The feature that helps in monitoring Azure resources for abnormal activity and potential threats is Azure Security Center. This tool is central to Azure's security posture management, providing users with a comprehensive view of their security status across various Azure resources. Azure Security Center continuously assesses the security state of resources and provides recommendations based on best practices. It utilizes advanced analytics and machine learning to detect anomalies and potential threats, enabling organizations to respond swiftly to any suspicious activities. It helps identify vulnerabilities and provides actionable insights, such as alerts regarding suspicious activity in virtual machines or unusual traffic patterns, enhancing an organization's overall security response. The other features mentioned serve different purposes within the Azure ecosystem. For instance, Azure Advisor offers personalized best practices recommendations for optimizing Azure resources, but it does not specifically monitor for security threats. Azure Policy helps enforce organizational standards by managing compliance across Azure resources but does not direct monitor activities. Azure Backup Center focuses on backup and disaster recovery solutions rather than threat detection or monitoring. Therefore, Azure Security Center is the correct choice for monitoring Azure resources for abnormal activity and potential threats, making it integral to an organization’s security framework in the cloud environment.

5. Which security feature is available in the free mode of Microsoft Defender for Cloud?

A. Threat protection alerts

B. Just-in-time (JIT) VM access to Azure virtual machines

C. Vulnerability scanning of virtual machines

D. Secure score

The option referring to the secure score is the correct answer because it is a key feature of Microsoft Defender for Cloud that is accessible in its free tier. The secure score provides organizations with a comprehensive assessment of their security posture across Azure resources and helps identify security risks. It offers actionable recommendations to enhance security levels and prioritize improvements based on the organization's specific environment. The secure score feature is valuable for organizations looking to establish best practices in security without incurring additional costs. It gives organizations visibility into how well they are adhering to security policies and provides a benchmark for improvement. The other features mentioned, such as threat protection alerts, just-in-time VM access, and vulnerability scanning, typically require a higher tier of service that includes additional capabilities and protections that go beyond what is provided for free. Garnering insights from the secure score can empower organizations to make informed security decisions and implement necessary changes effectively.

6. What are customers responsible for when evaluating security in a software as a service (SaaS) cloud services model?

A. operating systems

B. network controls

C. applications

D. accounts and identities

In the Software as a Service (SaaS) model, customers hold key responsibilities primarily concerning their accounts and identities. This includes managing user access, maintaining strong authentication practices, and ensuring that user accounts are secured against unauthorized access. Customers are tasked with defining roles and permissions for their users, as well as overseeing identity and access management to safeguard sensitive information processed within the SaaS applications. While aspects like operating systems, network controls, and applications are typically managed by the service provider in a SaaS environment, the responsibility for accounts and identities rests with the customer. This delineation is a crucial aspect of the shared responsibility model in cloud services, where the provider handles the infrastructure and platform while customers maintain control over their data, users, and identities. Understanding this division of responsibility helps organizations effectively secure their resources in the cloud.

7. Which tasks can be performed by Azure Active Directory (Azure AD) Identity Protection? Select all that apply.

A. Configure external access for partner organizations

B. Export risk detection to third-party utilities

C. Automate the detection and remediation of identity based-risks

D. Investigate risks that relate to user authentication

Azure Active Directory (Azure AD) Identity Protection is specifically designed to help organizations manage and mitigate risks associated with user identities. One of its primary features is the automation of identifying and responding to identity-based risks. This capability allows organizations to detect and remediate potential threats automatically, such as suspicious sign-in attempts or compromised accounts, thereby enhancing the security posture without requiring extensive manual intervention. Additionally, Azure AD Identity Protection provides tools to assist organizations in monitoring and investigating risks related to user authentication. Investigating authentication risks is crucial for understanding the nature and impact of potential security threats. Through risk detection, organizations can better protect their resources by understanding what types of risky behaviors or conditions exist. While Azure AD Identity Protection does offer automation and investigatory capabilities, it does not include functionalities such as configuring external access for partner organizations or exporting risk detection data to third-party utilities, which are outside its primary focus on identity and access management security. This highlights the importance of recognizing the specific functions and strengths of Azure AD Identity Protection within the broader Azure ecosystem.

8. Can Azure Active Directory (Azure AD) Identity Protection add users to groups based on the users' risk level?

A. Yes

B. No

C. Only for privileged users

D. Only for external users

Azure Active Directory (Azure AD) Identity Protection does not have the capability to automatically add users to groups based on their risk level. Its primary function is to detect potential vulnerabilities affecting your organization's identities, to investigate incidents, and to respond to detected issues by allowing you to take various actions to mitigate risks. The tool provides insights into user risk events and enables organizations to configure risk-based conditional access policies. These policies help in requiring additional authentication or blocking access for users deemed at high risk but do not extend to automatic group membership changes based on risk assessment. Understanding this function of Azure AD Identity Protection highlights its role in enhancing security but reinforces the fact that group management requires separate policies or actions outside of what Identity Protection directly offers. Therefore, the effective answer is that Azure AD Identity Protection cannot add users to groups based on risk levels, aligning with the selected response.

9. What action is required to create cases in the Case dashboard?

A. Triage

B. Investigate

C. Action

D. Review

Creating cases in the Case dashboard primarily involves the investigation phase. This action is fundamental to the process because it allows users to thoroughly analyze incidents or alerts that have been detected within a system. During investigation, relevant evidence and context are gathered, which informs the creation of a case. This is where users assess the situation, identify affected resources, and determine the necessary responses. Effective investigation leads to well-documented cases that can be assigned for further action, escalation, or resolution. Consequently, without conducting an investigation, the necessary details for a case would be missing, making it challenging to understand the situation or take appropriate measures. The other options pertain to stages of incident management but are not specifically tied to the initial action of creating a case in the dashboard. Triage focuses on prioritizing incidents, while reviewing involves looking over data post-investigation. Thus, investigation is the correct foundational step necessary for case creation.

10. Which privacy principle of Microsoft ensures that individuals have control over their personal information?

A. Transparency

B. Control

C. Security

D. Integrity

The principle that ensures individuals have control over their personal information is indeed highlighted by the concept of Control. This principle revolves around empowering users by giving them the ability to manage their own data. It emphasizes the importance of consent and choice regarding how personal data is collected, used, and shared. By applying this principle, Microsoft ensures that users can decide what information they want to share, with whom, and for what purpose, thereby reinforcing their autonomy over personal data. Other principles, such as Transparency, relate to informing users about how their data is used, which supports informed consent but does not inherently grant control. Security focuses on protecting data from unauthorized access and breaches, ensuring that personal information is safeguarded, while Integrity emphasizes the accuracy and reliability of data. While these principles are important for a comprehensive data privacy framework, Control specifically addresses the user's power over their personal information.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://microsoftsecuritycomplianceandidentitydundamentals-sc900.examzify.com

We wish you the very best on your exam journey. You've got this!