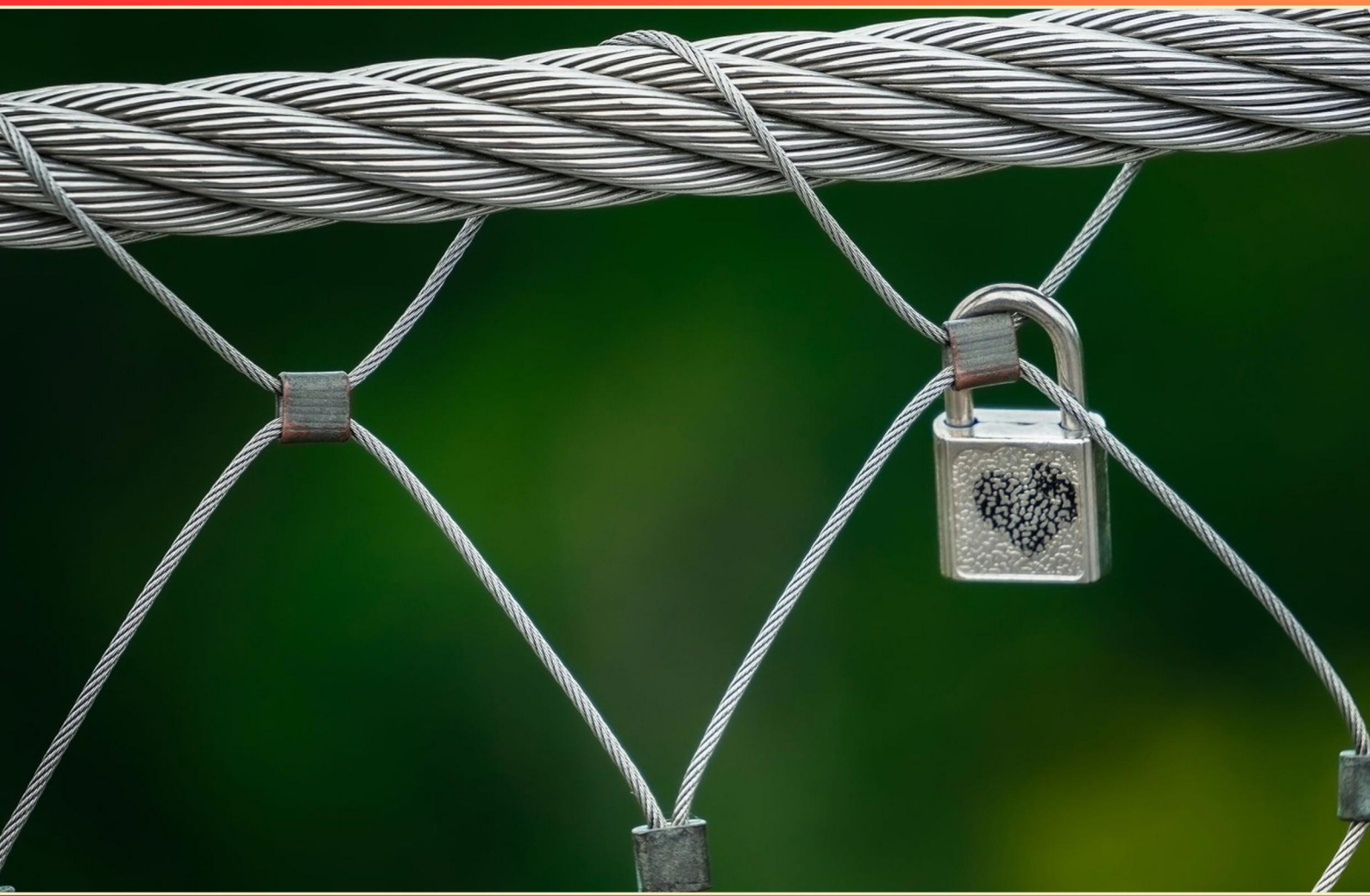
MICROSOFT SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS (SC-900) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://microsoftsecuritycomplianceandidentitydundamentals-sc900.examzify.com

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. 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.

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. 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 of the following can sensitivity labels apply to a Microsoft Word document?**

   A. A watermark

   B. A password

   C. A digital signature

   D. An index

2. **Which Microsoft 365 compliance feature allows for automatic encryption of content based on specific conditions?**

   A. Content Search

   B. Retention policies

   C. Sensitivity labels

   D. eDiscovery

3. **Can Network Security Groups (NSGs) deny outbound traffic to the internet?**

   A. Yes

   B. No

   C. Only for secure protocols

   D. Depends on configuration

4. **In Azure Active Directory (Azure AD) Identity Protection, does a user risk represent the probability that a given identity or account is compromised?**

   A. Yes

   B. No

   C. Not applicable

   D. Only for administrative accounts

5. **To which type of resource can Azure Bastion provide secure access?**

   A. Azure Files

   B. Azure SQL Managed Instances

   C. Azure virtual machines

   D. Azure App Service

6. Are global administrators exempt from conditional access policies?

A. Yes

B. No

C. Only if they are on a trusted device

D. Only temporarily

7. Can Azure Defender detect vulnerabilities and threats for Azure Storage?

A. Yes

B. No

C. Only for specific types of storage

D. Only for third-party storage

8. Can conditional access policies block access based on user location?

A. Yes

B. No

C. Only for external users

D. Only for administrators

9. Which of the following is NOT a guiding principle of Zero Trust?

A. Assume breach

B. Verify explicitly

C. Trust but verify

D. Least privilege access

10. Can Network Security Groups (NSGs) deny inbound traffic from the internet?

A. Yes

B. No

C. Sometimes

D. Only for specific ports

Answers

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

Explanations

1. Which of the following can sensitivity labels apply to a Microsoft Word document?

A. A watermark

B. A password

C. A digital signature

D. An index

Sensitivity labels in Microsoft 365 are used to classify and protect sensitive information within documents and emails. When applied to a Microsoft Word document, sensitivity labels can enforce specific protections and policies, such as applying watermarks to indicate the sensitivity level of the document. Applying a watermark is a visible indication that can inform users about the confidentiality of the document, helping to ensure that the content is treated appropriately. This is especially important for sensitive information, as it continuously reminds users of the document's classification, even when printed or shared. The other options, while they have their own security and usability functions, do not have the same direct link to sensitivity labeling. For instance, a password protects access to a document but does not indicate its sensitivity level. A digital signature verifies the authenticity and integrity of a document but is not related to its classification or how it should be handled based on its sensitivity. An index, while useful for navigation and organization within documents, does not impact the document's sensitivity or classification either. Thus, the most appropriate application of sensitivity labels in this context is through watermarks, enhancing document awareness regarding sensitivity levels.

2. Which Microsoft 365 compliance feature allows for automatic encryption of content based on specific conditions?

A. Content Search

B. Retention policies

C. Sensitivity labels

D. eDiscovery

The feature that allows for automatic encryption of content based on specific conditions is sensitivity labels. Sensitivity labels are an integral part of the Microsoft 365 compliance framework, enabling organizations to classify, label, and protect their sensitive information. When defined policies are applied, these labels can trigger automatic encryption of documents and emails based on the labels assigned. For instance, if an organization wants to ensure that certain types of documents, such as those containing personally identifiable information (PII), are encrypted to meet compliance requirements, they can set up sensitivity labels that enforce encryption when those labels are applied to documents. This automatic approach helps streamline compliance with regulations such as GDPR or HIPAA. Other options, such as content search, retention policies, and eDiscovery, have different functions related to compliance and data governance. Content search is focused on searching for content across Microsoft 365, retention policies manage the lifecycle of data but do not provide encryption, and eDiscovery is used to identify and manage legal holds on data for legal investigations. These functions are crucial but do not specifically address the automatic encryption of content like sensitivity labels do.

3. Can Network Security Groups (NSGs) deny outbound traffic to the internet?

A. Yes

B. No

C. Only for secure protocols

D. Depends on configuration

Network Security Groups (NSGs) can indeed deny outbound traffic to the internet. NSGs are used in Azure to control inbound and outbound traffic to network interfaces, VMs, and subnets. They contain a list of rules that can explicitly allow or deny traffic based on specific conditions such as IP addresses, ports, and protocols. When a rule is configured to deny outbound traffic, it effectively blocks any connections that match the rule. This allows for very granular control over the traffic flow from your resources in the Azure environment. Organizations can use NSGs to enforce security policies, limit exposure to the internet, and protect resources from unauthorized access or data exfiltration. While NSGs can allow or deny traffic depending on how they are configured, they can clearly be set to deny specific outbound traffic to the internet, which is a key feature for maintaining secure network boundaries.

4. In Azure Active Directory (Azure AD) Identity Protection, does a user risk represent the probability that a given identity or account is compromised?

A. Yes

B. No

C. Not applicable

D. Only for administrative accounts

A user risk in Azure Active Directory Identity Protection indeed represents the probability that a particular identity or account may be compromised. This concept is fundamental to identity management and security within Azure AD. User risk assessments are based on various signals, including sign-in behavior, the location of the sign-in, and other contextual factors that indicate whether an account might be at risk of unauthorized access. Azure AD uses machine learning and heuristics to analyze this data, generating a risk level that helps security administrators identify potentially compromised accounts and take appropriate actions, such as requiring password resets or multifactor authentication. Recognizing user risk is critical for implementing proactive security measures, enabling organizations to respond effectively to potential breaches and mitigate risks associated with compromised accounts. By assessing risks, organizations can better protect sensitive information and maintain compliance with security policies and regulations.

5. To which type of resource can Azure Bastion provide secure access?

A. Azure Files

B. Azure SQL Managed Instances

C. Azure virtual machines

D. Azure App Service

Azure Bastion is a service within Microsoft Azure that provides secure and seamless RDP (Remote Desktop Protocol) and SSH (Secure Shell) access to virtual machines directly through the Azure portal. This eliminates the need for a public IP address on the virtual machines, thus enhancing security by preventing exposure to the internet. When using Azure Bastion, users can connect to their Azure virtual machines without having to manage jump boxes or other intermediate solutions, thus simplifying the architecture for remote access. This secure, fully managed service integrates directly with Azure, allowing users to connect to their VMs using a web browser, which further emphasizes accessibility and ease of use. Understanding how Azure Bastion works in relation to other Azure resources is important. Azure Files, Azure SQL Managed Instances, and Azure App Service have their own distinct access and management methods, such as direct file sharing, Azure Data Studio, or app service environments, which do not require the same secure connectivity provided by Azure Bastion. Therefore, the primary functionality of Azure Bastion is specifically tailored to Azure virtual machines, making them the correct choice for secure access via this service.

6. Are global administrators exempt from conditional access policies?

A. Yes

B. No

C. Only if they are on a trusted device

D. Only temporarily

Global administrators are not exempt from conditional access policies, which is why the answer is B. Conditional access policies are designed to enforce security measures regardless of a user's administrative role within an organization. This ensures that even those with the highest level of privileges, such as global administrators, are subject to the same security requirements as regular users. The rationale behind this policy is to protect sensitive data and resources from potential risks or vulnerabilities, including those that could arise from compromised administrator accounts. By applying conditional access to all users, organizations can help reduce the attack surface and enforce consistent security policies across the board. This approach aligns with the broader principle of "least privilege," emphasizing that no user should have unrestricted access without passing established security checks, thereby maintaining the integrity and confidentiality of the organization's resources.

7. Can Azure Defender detect vulnerabilities and threats for Azure Storage?

A. Yes

B. No

C. Only for specific types of storage

D. Only for third-party storage

Azure Defender is indeed equipped to detect vulnerabilities and threats for Azure Storage. It provides continuous security assessment and enhances the security posture of Azure Storage by identifying potential vulnerabilities, misconfigurations, and threats. This includes monitoring for unusual access patterns or behavior that might indicate a security breach or attack. Azure Defender applies various security measures, such as threat intelligence, behavioral analytics, and machine learning, to protect resources within Azure Storage. It alerts you to detected threats and provides actionable recommendations to mitigate risks, ensuring that your storage accounts are secure from both internal and external threats. Considering this functionality, the answer that Azure Defender can detect vulnerabilities and threats related to Azure Storage is accurate and reflects Azure's commitment to providing robust security features in its ecosystem.

8. Can conditional access policies block access based on user location?

A. Yes

B. No

C. Only for external users

D. Only for administrators

Conditional access policies in Microsoft Azure Active Directory (Azure AD) are designed to enhance security by allowing organizations to set and enforce access rules based on specific conditions. One of these conditions includes the user's location. By utilizing conditional access policies, an organization can specify that certain applications or resources are accessible only from specific networks or geographical locations. For instance, a business might allow access to sensitive data only from within the corporate network or deny access from regions that are deemed high-risk. This capability provides a powerful tool for managing security and ensuring that only trusted, intended locations can access critical resources. As a result, this feature not only helps protect against unauthorized access but also facilitates compliance with various regulatory requirements regarding data security and user information. In contrast, other choices such as limiting to only external users or administrators do not align with the broader functionality of conditional access policies, which are applicable to any user based on their defined access conditions.

9. Which of the following is NOT a guiding principle of Zero Trust?

A. Assume breach

B. Verify explicitly

C. Trust but verify

D. Least privilege access

The principle of "Trust but verify" is not a guiding tenet of Zero Trust. Instead, Zero Trust emphasizes that organizations should never implicitly trust any user or system, even if they are inside the network perimeter. The philosophy of Zero Trust is centered around the idea of continuous verification and validation. In a Zero Trust model: - "Assume breach" suggests that organizations should operate with the mindset that a breach could occur at any time, focusing on preventing lateral movement within the network. - "Verify explicitly" highlights the necessity to authenticate and authorize every access request based on various factors, including user identity, device health, and location. - "Least privilege access" means granting users only the permissions necessary to perform their jobs, minimizing the risk of potential harm from compromised accounts. These principles are crucial for establishing robust security infrastructure in today's increasingly complex threat landscape. In contrast, the concept of "Trust but verify" implies a level of initial trust, which contradicts the foundational premise of Zero Trust.

10. Can Network Security Groups (NSGs) deny inbound traffic from the internet?

A. Yes

B. No

C. Sometimes

D. Only for specific ports

Network Security Groups (NSGs) are an essential component of Microsoft Azure's security framework, designed to control network traffic to and from Azure resources. The functionality of NSGs allows for the creation of rules that can permit or deny inbound and outbound traffic based on specific criteria such as source IP address, destination IP address, port number, and protocol. When the question pertains to whether NSGs can deny inbound traffic from the internet, the correct response highlights an important feature of NSGs: they can indeed be configured to deny specific traffic, including that which originates from the internet. By default, an NSG allows all inbound traffic unless explicitly denied, enabling administrators to customize security posture according to their requirements. By defining rules, you can specify that traffic from the internet (with a source of 0.0.0.0/0) should be denied, effectively restricting external access to your resources. The capability to deny specific types of traffic enhances security by allowing organizations to enforce strict access controls, ensuring that only legitimate and necessary traffic reaches Azure resources. Therefore, the answer accurately reflects the functionality of NSGs in managing and securing inbound traffic from the internet.

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!