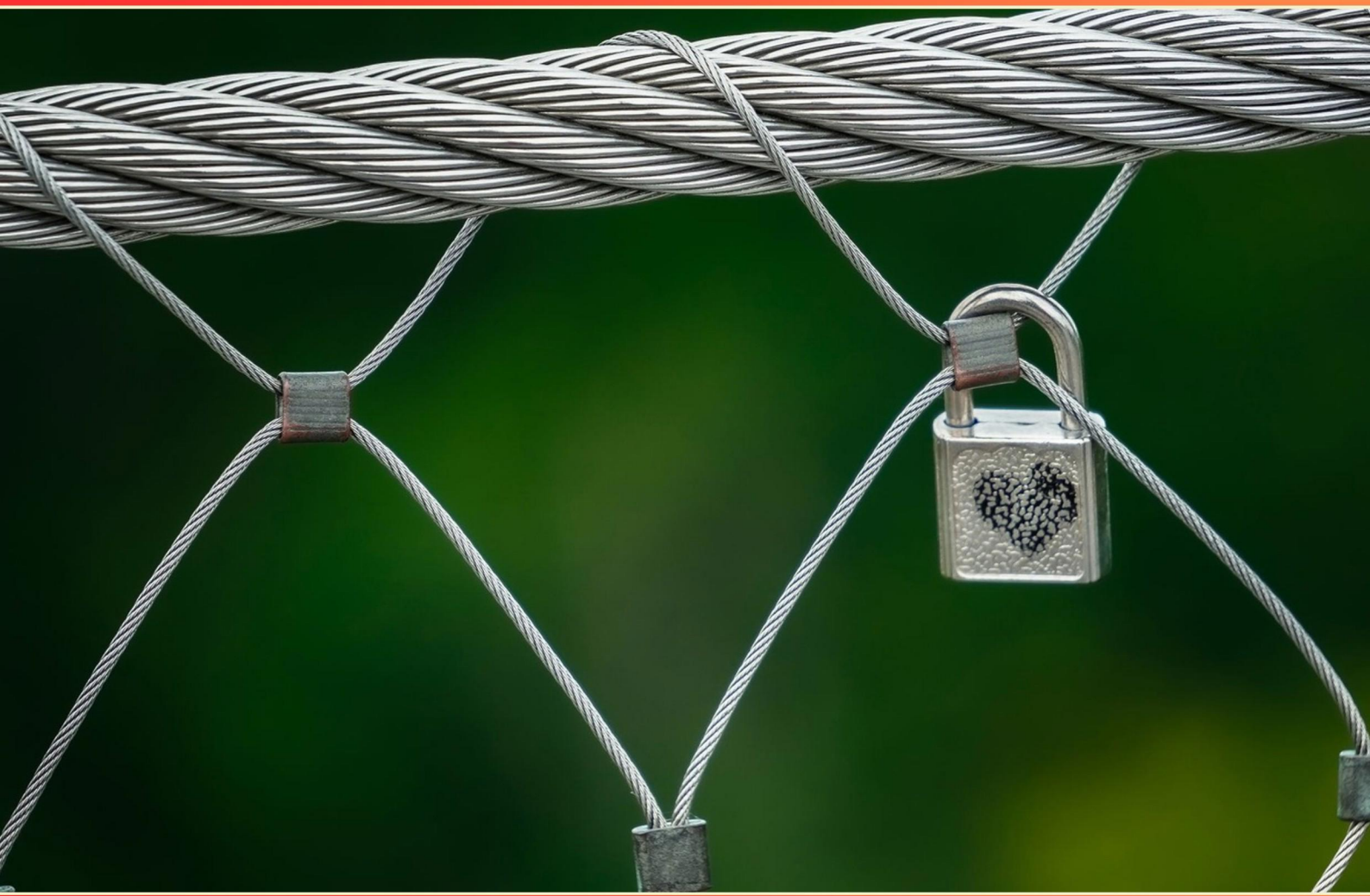
MICROSOFT SECURITY, COMPLIANCE, AND IDENTITY FUNDAMENTALS (SC-900) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://microsoftsecuritycomplianceandidentitydundamentals-sc900.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. **In the Microsoft 365 Defender portal, an incident is a collection of correlated _____**

   A. alerts

   B. events

   C. vulnerabilities

   D. Microsoft Secure Score improvement actions

2. **Are conditional access policies evaluated before a user is authenticated?**

   A. Yes

   B. No

   C. Only for new users

   D. Only for devices

3. **Compliance Manager can be directly accessed from which of the following?**

   A. Microsoft 365 admin center

   B. Microsoft 365 Defender portal

   C. Microsoft Support portal

   D. Microsoft Purview

4. **In Software as a Service (SaaS), who is responsible for applying service packs to the application?**

   A. The organization

   B. The cloud provider

   C. Both the organization and provider

   D. No responsibility

5. **Which solution can scan email attachments for malware before forwarding?**

   A. Microsoft Defender for Office 365

   B. Microsoft Defender Antivirus

   C. Microsoft Defender for Identity

   D. Microsoft Defender for Endpoint

SAMPLE

6. Which feature in Microsoft 365 helps to safeguard sensitive information and reduce security risks associated with external sharing?

A. Compliance Manager

B. Information protection

C. Data Loss Prevention (DLP)

D. Azure Information Protection

7. Which capability of Microsoft Intune allows for managing personal devices in an organization?

A. Provisioning

B. Device management

C. Security updates

D. Compliance monitoring

8. What compliance feature is best for identifying employee resumes in documents?

A. Pre-trained classifiers

B. Activity explorer

C. eDiscovery

D. Content explorer

9. What is the primary purpose of Multi-Factor Authentication (MFA) in identity protection?

A. To store user credentials securely

B. To provide users with single sign-on capabilities

C. To enhance security by requiring two or more verification methods

D. To track user access to resources

10. What measures a company's progress in reducing risks around data protection and regulatory standards?

A. Compliance score

B. Regulatory report

C. Risk assessment report

D. Data protection plan

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. In the Microsoft 365 Defender portal, an incident is a collection of correlated _____

A. alerts

B. events

C. vulnerabilities

D. Microsoft Secure Score improvement actions

In the Microsoft 365 Defender portal, an incident is a collection of correlated alerts. An alert represents a potential security issue detected by the Microsoft 365 Defender solutions, such as Microsoft Defender for Endpoint or Microsoft Defender for Office 365. When multiple alerts arise from the same threat or tactic, they are grouped into an incident to provide a comprehensive view of the threat landscape and facilitate coordinated response actions. This allows security teams to prioritize their efforts based on the severity and nature of the alerts, improving the incident response process. Events refer to individual occurrences within a system, while vulnerabilities pertain to weaknesses that may potentially be exploited by threats; both concepts differ from the aggregation of alerts into incidents. The Microsoft Secure Score improvement actions indicate how organizations can enhance their security posture but are not themselves incidents related to the detection of threats. Therefore, alerts are the critical elements that compile into an incident within the context of Microsoft 365 Defender.

2. Are conditional access policies evaluated before a user is authenticated?

A. Yes

B. No

C. Only for new users

D. Only for devices

Conditional access policies are indeed evaluated after a user has been authenticated. The purpose of these policies is to provide an additional layer of security by determining whether a user can access a specific resource based on conditions such as user location, device compliance, risk level, and more. Once a user attempts to access a resource, they go through the authentication process. After successful authentication, the conditional access policies are then evaluated to determine if the access can proceed or if additional measures, such as multifactor authentication or restrictions, should be applied. This sequence ensures that only users who meet the necessary conditions can access certain resources, thereby securing access based on predefined security requirements. By placing the evaluation after authentication, organizations can implement more stringent access controls tailored to their security posture while ensuring that users can successfully authenticate in the first place. This design reflects a balance between user experience and security.

SAMPLE

3. Compliance Manager can be directly accessed from which of the following?

A. Microsoft 365 admin center

B. Microsoft 365 Defender portal

C. Microsoft Support portal

D. Microsoft Purview

Compliance Manager is a feature that helps organizations manage their compliance requirements and assess their compliance posture. It offers tools for building workflows around compliance and provides guidance based on various regulatory standards and frameworks. The most direct access to Compliance Manager is through Microsoft Purview. Microsoft Purview encompasses various compliance solutions, including Compliance Manager, which is designed to help organizations efficiently manage their data governance, compliance, risk management, and information protection. Microsoft Purview acts as the centralized hub for compliance solutions, making it the optimal choice for accessing Compliance Manager. This access allows users to leverage the comprehensive tools available within Purview that enhance their compliance efforts. While the Microsoft 365 admin center is the management interface for overall Microsoft 365 services, it does not provide direct access to Compliance Manager. The Microsoft 365 Defender portal focuses on security solutions, and the Microsoft Support portal is primarily aimed at providing support resources rather than compliance management tools. Therefore, these options do not provide the specialized access that comes with Microsoft Purview.

4. In Software as a Service (SaaS), who is responsible for applying service packs to the application?

A. The organization

B. The cloud provider

C. Both the organization and provider

D. No responsibility

In a Software as a Service (SaaS) model, the responsibility for applying service packs and maintaining the software application generally resides with the cloud provider. This model allows organizations to use software without needing to manage the underlying infrastructure and application updates themselves. The provider ensures that the software is kept up to date with the latest service packs, security patches, and features. Organizations utilizing SaaS solutions typically focus on configuring and using the application rather than managing its maintenance and updates. This allows them to benefit from continual improvements and security updates without directly managing those processes. In contrast, when it comes to other service models like Infrastructure as a Service (IaaS) or Platform as a Service (PaaS), the responsibility of updates can vary, placing a greater burden on the organization to manage patches and updates. However, SaaS providers take care of these aspects, making it more efficient and less resource-intensive for users.

SAMPLE

5. Which solution can scan email attachments for malware before forwarding?

A. Microsoft Defender for Office 365

B. Microsoft Defender Antivirus

C. Microsoft Defender for Identity

D. Microsoft Defender for Endpoint

Microsoft Defender for Office 365 is designed specifically to protect against threats across Microsoft 365 applications, including email. It features robust capabilities to detect and mitigate malware contained within email attachments. By scanning attachments at the moment messages are processed, it can identify and block potentially harmful content before forwarding, thus providing a layer of security that helps prevent data breaches and other security incidents. This solution leverages advanced threat protection techniques, such as machine learning and heuristics, to analyze attachments and ensure only safe content reaches the recipient. It also includes features for phishing detection and spam filtering, making it an essential component for organizations looking to secure their email communications effectively. Other options, while part of the broader Microsoft security ecosystem, are tailored for distinct purposes. Microsoft Defender Antivirus focuses on malware detection and remediation at the device level, Microsoft Defender for Identity is aimed at identity and access management threats, and Microsoft Defender for Endpoint provides protection against security threats targeting devices and applications. None of these solutions specifically target the email attachment scanning functionality that Microsoft Defender for Office 365 excels at.

6. Which feature in Microsoft 365 helps to safeguard sensitive information and reduce security risks associated with external sharing?

A. Compliance Manager

B. Information protection

C. Data Loss Prevention (DLP)

D. Azure Information Protection

Data Loss Prevention (DLP) is a critical feature in Microsoft 365 designed to help organizations protect sensitive information from being inadvertently shared with unauthorized users, especially during external sharing. DLP policies enable administrators to identify and monitor sensitive data, such as personally identifiable information (PII), credit card numbers, or health information, and apply specific actions when this data is shared outside the organization. For example, with DLP, if a user attempts to share a document that contains sensitive information, the policy can prevent the action, notify the user about the violation, or even encrypt the data before it is shared. This proactive approach not only helps meet compliance requirements but also significantly reduces the risk of data breaches and unintentional loss of sensitive information. By implementing DLP, organizations can take a strategic stance on managing their data security, ensuring that sensitive information is handled properly throughout its lifecycle, particularly in scenarios involving external sharing. This makes DLP a vital tool for safeguarding data and managing security risks effectively.

SAMPLE

7. Which capability of Microsoft Intune allows for managing personal devices in an organization?

A. Provisioning

B. Device management

C. Security updates

D. Compliance monitoring

The capability of Microsoft Intune that allows for managing personal devices in an organization is related specifically to device management. Device management in Intune encompasses a range of functionalities that facilitate the administration of both corporate and personal devices within a management framework known as Mobile Device Management (MDM). This capability enables organizations to enforce policies, deploy applications, configure settings, and monitor device status to ensure compliance and security, regardless of whether the devices are owned by the organization or are personal devices used for work purposes (commonly referred to as BYOD - Bring Your Own Device). By implementing device management policies through Intune, organizations can enforce security measures, such as requiring passcodes, encrypting data, and managing access to corporate resources. This is crucial in a modern workplace where employees increasingly use their personal devices to perform work functions, necessitating a reliable way to ensure that these devices meet organizational security standards without infringing on users' privacy. In contrast, provisioning refers to the initial setup or configuration of devices, which does not exclusively pertain to ongoing management. Security updates are crucial for protecting devices but do not encompass the broader aspect of management and policy enforcement. Compliance monitoring is important for ensuring devices adhere to organizational policies but is a specific function within the overall device management capabilities

8. What compliance feature is best for identifying employee resumes in documents?

A. Pre-trained classifiers

B. Activity explorer

C. eDiscovery

D. Content explorer

The best compliance feature for identifying employee resumes in documents is the use of pre-trained classifiers. Pre-trained classifiers are machine learning models that have been specifically designed to recognize and categorize certain types of content based on training from existing data. In the case of employee resumes, these classifiers can effectively scan through various documents and accurately identify instances of resumes based on patterns and keywords they have been trained on. By utilizing pre-trained classifiers, organizations can efficiently manage and organize sensitive content within their data, making it easier to ensure compliance with regulations related to data privacy and protection. This automated approach not only saves time but also improves the accuracy of identifying relevant documents, which is crucial for compliance monitoring and reporting. Other options like Activity explorer, eDiscovery, and Content explorer serve different purposes in compliance and data management. For instance, Activity explorer focuses on tracking user activities within an organization, eDiscovery is used for finding and managing electronically stored information during legal investigations, and Content explorer is typically concerned with visualizing and understanding content within a data set. While these tools are valuable in their respective areas, they do not specifically target the identification of employee resumes as efficiently as pre-trained classifiers.

SAMPLE

9. What is the primary purpose of Multi-Factor Authentication (MFA) in identity protection?

A. To store user credentials securely

B. To provide users with single sign-on capabilities

C. To enhance security by requiring two or more verification methods

D. To track user access to resources

The primary purpose of Multi-Factor Authentication (MFA) in identity protection is to enhance security by requiring two or more verification methods. MFA goes beyond just a username and password, which can be easily compromised, by adding additional layers of security. This typically includes something the user knows (like a password), something the user has (like a mobile device or hardware token), and/or something the user is (like biometric data). By implementing MFA, organizations can significantly reduce the risk of unauthorized access to sensitive systems and data. Even if a user's password is stolen or guessed, the attacker would still need the second (or additional) form of verification to gain access. This additional requirement makes it much more difficult for unauthorized users to breach accounts, thereby strengthening the overall security posture of an organization. Other options, while relating to identity management, do not directly address the core function of MFA. Storing user credentials securely pertains to password management practices, single sign-on focuses on user convenience with access management, and tracking user access is more about auditing and monitoring rather than authentication processes.

10. What measures a company's progress in reducing risks around data protection and regulatory standards?

A. Compliance score

B. Regulatory report

C. Risk assessment report

D. Data protection plan

The compliance score is a crucial metric for measuring a company's progress in reducing risks associated with data protection and adhering to regulatory standards. This score is typically derived from the assessment of the organization's security controls, practices, and policies against established benchmarks or compliance frameworks. It quantifies how well a company meets various regulatory requirements and identifies areas that need improvement. A compliance score not only reflects an organization's current standing but also provides insights into its ongoing efforts to enhance data integrity, confidentiality, and availability. It can serve as a valuable tool for stakeholders to evaluate the effectiveness of implemented security measures and strategies focused on minimizing risks in data management and regulatory adherence. In contrast, a regulatory report typically provides a snapshot of compliance for a specific period or initiative but does not measure ongoing progress over time. Similarly, a risk assessment report identifies potential risks and vulnerabilities but does not serve as a direct measure of how effectively a company has improved its compliance status. Lastly, a data protection plan outlines strategies and objectives but does not quantify progress or success in terms of compliance score.

SAMPLE

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!

SAMPLE