ISACA CYBERSECURITY FUNDAMENTALS CERTIFICATION PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://isaca-cybersecurity.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. What is the main focus of a Business Continuity Plan (BCP)?

A. To enhance network performance

B. To ensure uninterrupted employee productivity

C. To recover and restore interrupted critical functions

D. To conduct regular vulnerability assessments

2. Which of the following is a potential issue with remote users' computers?

A. Excessive file sharing

B. Inadequate physical security

C. Overuse of system resources

D. High bandwidth usage

3. How do differential backups accumulate changes over time?

A. By copying all files that have changed since any backup

B. By copying all files that remain unchanged

C. By copying files that differ from the previous incremental backup

D. By copying only files that have changed since the last full backup

4. What is malware?

A. Software used for system optimization

B. Software designed to disrupt functioning without consent

C. Software approved by the user

D. Software that is easily removable

5. What does a digital signature provide to the recipient?

A. Assurance of data compression

B. Verification of data integrity and sender's identity

C. Instantaneous message delivery confirmation

D. Ability to change the data within the signature

6. During which phase of the IRP is the incident management team activated?

A. Investigation

B. Containment

C. Mitigation

D. Preparedness

SAMPLE

7. Which of the following is NOT one of the NIST functions to protect digital assets?

A. Identify

B. Protect

C. Execute

D. Recover

8. What do attack-signature-detection tools focus on identifying?

A. Unusual network traffic

B. Specific sequences of unauthorized access attempts

C. Trends in system performance

D. Data loss incidents

9. What is the primary purpose of anti-forensics in cybersecurity?

A. To enhance data security

B. To manipulate or erase digital data

C. To facilitate digital investigations

D. To speed up data recovery

10. What characterizes a dual-homed firewall?

A. It connects multiple LANs

B. It has multiple network cards

C. It is the simplest firewall configuration

D. It manages a single point of access

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the main focus of a Business Continuity Plan (BCP)?

A. To enhance network performance

B. To ensure uninterrupted employee productivity

C. To recover and restore interrupted critical functions

D. To conduct regular vulnerability assessments

The main focus of a Business Continuity Plan (BCP) is to recover and restore interrupted critical functions. A BCP is designed to ensure that an organization can continue operating and recover quickly in the face of disruptions, such as natural disasters, cyberattacks, or other emergencies. By establishing protocols, procedures, and resources ahead of time, a BCP ensures that essential business operations can be maintained or swiftly resumed. This focus on recovery emphasizes the importance of identifying critical business functions and the resources required to support them. The plan typically outlines strategies for keeping these functions operational during a crisis, including the restoration of personnel, infrastructure, technology, and communication. In contrast, enhancing network performance, ensuring uninterrupted employee productivity, and conducting regular vulnerability assessments are all important aspects of cybersecurity and operational management, but they do not encapsulate the primary goal of a BCP, which is centered on recovery in the event of significant disruptions.

2. Which of the following is a potential issue with remote users' computers?

A. Excessive file sharing

B. Inadequate physical security

C. Overuse of system resources

D. High bandwidth usage

Inadequate physical security is a significant concern for remote users' computers because these devices are often used outside of a controlled environment, such as an office or secure facility. When employees work remotely, their computers can be vulnerable to theft or unauthorized access, especially if they are left unattended in public places like coffee shops or libraries. Without the protections typically found in secured office spaces—such as access control systems, surveillance cameras, and secure storage—remote users must rely on individual discipline and informal measures to protect sensitive information. This lack of physical security can lead to data breaches or compromise critical business information if devices are lost or stolen. In contrast, while excessive file sharing, overuse of system resources, and high bandwidth usage are issues that can affect remote work, they do not pose the same immediate risk to physical data security as inadequate physical security does. Issues like file sharing primarily relate to data governance and usage policies, system resource management concerns impact performance, and high bandwidth usage deals with network efficiency rather than direct threats to the integrity of the hardware itself.

SAMPLE

3. How do differential backups accumulate changes over time?

A. By copying all files that have changed since any backup

B. By copying all files that remain unchanged

C. By copying files that differ from the previous incremental backup

D. By copying only files that have changed since the last full backup

Differential backups are designed to streamline the backup process by focusing on changes made since the last full backup. This method involves copying only the data that has been modified or created after the most recent full backup. As a result, each differential backup captures all the changes that have occurred, allowing for a more efficient restoration process if needed. Throughout the period between full backups, as new data is added or existing data is modified, these changes are recognized and included in each subsequent differential backup. This is particularly beneficial because, during a restoration, only the last full backup and the most recent differential backup need to be accessed to fully recover the system. This contrasts with other backup methods, such as incremental backups, which only capture changes made since the last backup (full or incremental) and can require restoring multiple sets of backups to achieve full data recovery. In the context of the other options, copying all files changed since any backup would lead to redundancy and larger storage requirements. Copying unchanged files does not align with the goal of effective backups and would waste resources. Focusing solely on files that differ from the previous incremental backup would not capture all changes since the last full backup, which is critical for a comprehensive recovery solution. Overall, the approach of copying only the files

4. What is malware?

A. Software used for system optimization

B. Software designed to disrupt functioning without consent

C. Software approved by the user

D. Software that is easily removable

Malware, short for malicious software, is specifically designed to disrupt, damage, or gain unauthorized access to computer systems or networks. This definition captures the essence of its intent and functionality, emphasizing that malware operates without the consent or knowledge of the user. It encompasses various types of harmful software, including viruses, worms, trojans, ransomware, and spyware, all of which aim to compromise system integrity or steal sensitive information. The key characteristic that differentiates malware from benign software is that it is built with malicious intent, seeking to exploit vulnerabilities in systems or user behavior to achieve its objectives. The other options do not align with the definition of malware. Software used for system optimization works to improve performance and efficiency, often with the user's consent. Software approved by the user would imply a positive, consent-driven interaction, which is contrary to the aims of malware. Lastly, software that is easily removable suggests a non-harmful or benign nature, whereas many forms of malware can be deeply embedded in systems, making them challenging to detect and remove. This underscores the critical nature of understanding malware's purpose and the risks it poses to cybersecurity.

SAMPLE

5. What does a digital signature provide to the recipient?

A. Assurance of data compression

B. Verification of data integrity and sender's identity

C. Instantaneous message delivery confirmation

D. Ability to change the data within the signature

A digital signature serves as a cryptographic mechanism that allows recipients to confirm both the integrity of the data and the identity of the sender. When a sender creates a digital signature using their private key, the signature is unique to the data being sent. This means that if even a single bit of the data changes, the digital signature will no longer be valid when checked with the sender's public key. Verification of data integrity is crucial because it ensures that the message has not been altered in transit. A valid digital signature provides assurance that the message received is exactly what the sender intended to send. Additionally, a digital signature helps establish the sender's identity by providing a means for the recipient to authenticate that the signature indeed comes from the purported sender. This is essential in preventing impersonation and ensuring trust in digital communications. The other options do not accurately represent the functions of a digital signature. Data compression is unrelated to digital signatures, instantaneous message delivery is a characteristic of transmission methods rather than security features, and a digital signature does not permit changes to the data—it actually ensures that any changes can be detected.

6. During which phase of the IRP is the incident management team activated?

A. Investigation

B. Containment

C. Mitigation

D. Preparedness

The correct answer pertains to the phase in the Incident Response Process (IRP) that is focused on containing the incident to prevent further damage or impact. During the containment phase, the incident management team is typically activated to assess the situation, implement strategies to limit the spread or impact of a security incident, and begin damage control measures. This execution is essential to ensure that any threats are neutralized and that normal operations can be restored as quickly as possible. This phase is crucial as it serves to minimize the potential impact on the organization while preparing to investigate the incident further or implement mitigation strategies. The preparedness phase happens earlier, centering on planning and training, rather than responding to incidents that have occurred. The investigation phase involves understanding the details of the incident post-containment, while mitigation details the actions taken to reduce the impact of the incident after immediate containment is established. Therefore, the activation of the incident management team is specifically aligned with the containment phase to handle incidents effectively and efficiently.

SAMPLE

7. Which of the following is NOT one of the NIST functions to protect digital assets?

A. Identify

B. Protect

C. Execute

D. Recover

The NIST Cybersecurity Framework outlines five core functions aimed at helping organizations manage and mitigate cybersecurity risks, which are Identify, Protect, Detect, Respond, and Recover. Among these, "Execute" does not appear as one of the defined functions. "Identify" involves understanding the organization's environment and the risks associated with their digital assets. "Protect" focuses on implementing safeguards to ensure the delivery of critical infrastructure services. "Recover" pertains to maintaining plans for resilience and restoring capabilities or services after a cybersecurity incident. Since "Execute" is not one of these recognized functions, it stands out as the option that does not fit within the NIST framework for safeguarding digital assets. This distinction reinforces the importance of understanding the framework's structure and its focus on systematic approaches to cybersecurity risk management.

8. What do attack-signature-detection tools focus on identifying?

A. Unusual network traffic

B. Specific sequences of unauthorized access attempts

C. Trends in system performance

D. Data loss incidents

Attack-signature-detection tools are specifically designed to identify patterns that match known attack signatures. These signatures are predefined characteristics or patterns of malicious activity, such as unique sequences of commands or data that are typically used during unauthorized access attempts. By recognizing these specific sequences, the tools can effectively alert security personnel to potential intrusions or attacks, allowing for a prompt response to mitigate threats. The emphasis on identifying specific unauthorized access attempts distinguishes this approach from broader monitoring techniques. For instance, while unusual network traffic could be a sign of an attack, it is not as definitive as recognizing a known attack signature. Similarly, trends in system performance and data loss incidents are commonly monitored for overall system health and security but do not directly relate to the identification of specific attack attempts. Therefore, focusing on specific unauthorized access attempts aligns precisely with the functionality of attack-signature-detection tools.

SAMPLE

9. What is the primary purpose of anti-forensics in cybersecurity?

A. To enhance data security

B. To manipulate or erase digital data

C. To facilitate digital investigations

D. To speed up data recovery

The primary purpose of anti-forensics in cybersecurity is to manipulate or erase digital data, which aligns with the correct answer. Anti-forensics techniques are employed by individuals seeking to obstruct or undermine forensic investigations. These techniques can include the use of various tools designed to erase or conceal data, making it difficult for investigators to recover information or understand the actions that took place on a system. By manipulating or erasing digital evidence, perpetrators of cybercrimes aim to hinder the investigation process and avoid detection or prosecution. In contrast, enhancing data security would involve measures that protect data integrity and confidentiality, which do not relate to anti-forensics. Facilitating digital investigations refers to methods and tools that assist investigators in uncovering and analyzing data, while speeding up data recovery focuses on the restoration of lost or damaged data, both of which come from a perspective of supporting rather than obstructing investigative processes. Therefore, these options are clearly distinct from the concept and intention behind anti-forensics, which is fundamentally about evading detection.

10. What characterizes a dual-homed firewall?

A. It connects multiple LANs

B. It has multiple network cards

C. It is the simplest firewall configuration

D. It manages a single point of access

A dual-homed firewall is characterized by having multiple network cards. This setup typically involves two network interfaces that connect to two distinct networks, often one to an internal trusted network and another to an external untrusted network, such as the internet. This configuration enhances security by creating a barrier between the two networks, allowing the firewall to control traffic between them effectively. The presence of multiple network cards is crucial because it facilitates the separation of network traffic. Each interface can be configured with different security policies, allowing for tailored rules that apply specifically to the internal or external network traffic. This distinction plays a vital role in preventing unauthorized access and monitoring data flow between networks. The other options, while related to firewall configurations, do not accurately describe the defining feature of a dual-homed firewall. Connecting multiple LANs is more characteristic of a multi-homed firewall, and stating that it is the simplest configuration does not hold since dual-homed setups tend to be more complex due to their separation of interfaces and associated rules. Additionally, a dual-homed firewall does not only manage a single point of access; it effectively manages traffic between two different network segments through its multiple interfaces.

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://isaca-cybersecurity.examzify.com

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

SAMPLE