CSX CYBERSECURITY FUNDAMENTALS PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS



VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://csxcybersecurityfund.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. **Which of the following backups includes only files that have changed since the last full backup?**

   A. Full backup

   B. Incremental backup

   C. Differential backup

   D. Mirror backup

2. **Which of the following is a method to control user traffic to the Internet?**

   A. Implementing data encryption

   B. Controlling user traffic bound toward the Internet

   C. Enhancing user permissions

   D. Creating multiple user accounts

3. **What type of security policy typically defines user responsibilities regarding data protection?**

   A. Acceptable Use Policy

   B. Privacy Policy

   C. Data Protection Policy

   D. Information Security Policy

4. **According to NIST, how is a threat defined?**

   A. A potential for data encryption

   B. A violation or imminent threat of violation of security policies

   C. A risk assessment for system vulnerabilities

   D. An attack on an unauthorized access point

5. **Which of the following concepts focuses on ensuring that sensitive data is not accessed by unauthorized users?**

   A. Access controls

   B. Encryption

   C. Network segmentation

   D. Firewall rules

SAMPLE

6. Which role is responsible for managing incidents and remediation within cybersecurity?

A. Cybersecurity analyst

B. Network administrator

C. Cybersecurity management

D. Technical support specialist

7. What is the purpose of the recovery process after a security incident?

A. To improve documentation practices

B. To ensure business processes continue

C. To re-evaluate the budget

D. To conduct post-incident reviews

8. Which components are included in identity management?

A. Data processing techniques

B. Directory services and user management capabilities

C. Artificial intelligence algorithms

D. Physical security measures

9. What type of management focuses on maintaining the performance of a network?

A. Fault management

B. Accounting management

C. Performance management

D. Security management

10. In risk management, which of the following is a proactive approach?

A. Ignoring potential threats

B. Continuously evaluating emerging risks

C. Post-event analysis

D. Implementing last-minute fixes

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which of the following backups includes only files that have changed since the last full backup?

A. Full backup

B. Incremental backup

C. Differential backup

D. Mirror backup

The correct answer is incremental backup. This type of backup is designed to capture only the files that have changed since the last full backup. By doing so, it optimizes storage space and reduces the time required to perform each backup session, as only new or modified files are included. This can be particularly advantageous in environments where data changes frequently, allowing for quicker backups and easier recovery. In contrast, a full backup involves copying all files, which can take significantly longer and require more storage space. A differential backup includes all files that have changed since the last full backup, meaning that it grows larger with each subsequent differential backup until the next full backup is taken. A mirror backup creates an exact copy of the data at the time of backup, which can omit older versions of files if they have been changed or deleted since the last backup, rather than just focusing on changes since the last full backup. These differences are key in understanding how incremental backups function within the larger context of data management and recovery strategies.

2. Which of the following is a method to control user traffic to the Internet?

A. Implementing data encryption

B. Controlling user traffic bound toward the Internet

C. Enhancing user permissions

D. Creating multiple user accounts

The method to control user traffic to the Internet involves actively managing the flow of data packets generated by users within an organization. This encompasses setting policies and rules about what types of traffic can exit the network, often through the use of firewalls, proxies, and network monitoring tools. The goal is to ensure that only authorized, necessary traffic reaches the Internet while blocking or restricting unauthorized access, thereby reducing the risk of data breaches and other cyber threats. In contrast, the other choices do not specifically target the control of traffic outbound to the Internet. Data encryption focuses on securing data in transit or at rest but does not regulate the permission-based access or traffic patterns towards the Internet. Enhancing user permissions relates to granting or restricting access to various resources within a system but does not directly impact user traffic. Creating multiple user accounts also does not influence how traffic flows to the Internet but is rather about user management and system organization. Thus, the key concept of controlling user traffic bound toward the Internet directly addresses the need for network security measures that manage and oversee the outgoing data, making it the most relevant and effective choice in this context.

SAMPLE

3. What type of security policy typically defines user responsibilities regarding data protection?

A. Acceptable Use Policy

B. Privacy Policy

C. Data Protection Policy

D. Information Security Policy

The Acceptable Use Policy is the type of security policy that typically defines user responsibilities regarding data protection. This policy sets the guidelines for how employees and users within an organization are expected to use its resources, including data, applications, and networks. It addresses what users can and cannot do, promoting responsible behavior in handling sensitive information. In an Acceptable Use Policy, responsibilities related to data protection are often articulated clearly, such as the proper handling of confidential information, the prohibition of unauthorized access to data, and the consequences of policy violations. By establishing these guidelines, organizations aim to ensure that all users are aware of their responsibilities in maintaining the integrity, confidentiality, and availability of data. Other types of policies, such as Privacy Policies or Data Protection Policies, focus more specifically on broader regulatory compliance or specific aspects of data handling rather than explicitly detailing user actions and responsibilities. The Information Security Policy encompasses overall security measures and frameworks within an organization but may not drill down into specific user behaviors like the Acceptable Use Policy does.

4. According to NIST, how is a threat defined?

A. A potential for data encryption

B. A violation or imminent threat of violation of security policies

C. A risk assessment for system vulnerabilities

D. An attack on an unauthorized access point

A threat, as defined by NIST, refers to any circumstance or event that has the potential to cause harm by violating or threatening to violate security policies. This definition emphasizes the aspect of potentiality, identifying threats as entities that can exploit vulnerabilities within a system or environment, leading to adverse consequences such as data breaches, loss of confidentiality, integrity, or availability. In this context, understanding the definition of a threat is crucial for implementing effective security measures and risk management practices. By identifying and assessing various threats, organizations can better prepare and respond to possible security incidents, ensuring that their security policies adequately protect assets against identified risks. This forms the foundation of creating a robust cybersecurity strategy. The other choices relate to different aspects of cybersecurity but do not align with the defined concept of a threat according to NIST. For example, a potential for data encryption suggests a method of securing data rather than a threat itself. Similarly, a risk assessment for system vulnerabilities pertains to identifying weaknesses within systems instead of focusing on threats, while an attack on an unauthorized access point describes an action rather than the potential for harm that constitutes a threat.

SAMPLE

5. Which of the following concepts focuses on ensuring that sensitive data is not accessed by unauthorized users?

A. Access controls

B. Encryption

C. Network segmentation

D. Firewall rules

Access controls are a fundamental concept in cybersecurity that focus on regulating who can view or use resources within a computing environment. They establish permissions based on user identity and roles, ensuring that only authorized individuals can access sensitive data. By implementing access controls, organizations can enforce security policies that prevent unauthorized access and protect confidential information from being misused or disclosed. This concept encompasses various methods, including role-based access control (RBAC), mandatory access control (MAC), and discretionary access control (DAC), each serving to restrict access based on predefined security rules. The goal is to guarantee that only those individuals with legitimate requirements to access certain information can do so, thereby enhancing the overall security posture against potential data breaches. In contrast, the other options, while important in their own rights, serve different purposes. Encryption protects data at rest or in transit by transforming it into a format that can only be read by those with the correct decryption key, but it does not manage who has access to that data. Network segmentation divides networks into smaller pieces to improve performance and security, but it alone doesn't control who can access sensitive data. Firewall rules act as a barrier to control incoming and outgoing traffic based on predetermined security rules, but they do not specifically address user access within applications or

6. Which role is responsible for managing incidents and remediation within cybersecurity?

A. Cybersecurity analyst

B. Network administrator

C. Cybersecurity management

D. Technical support specialist

The role responsible for managing incidents and remediation within cybersecurity is typically associated with cybersecurity management. This position involves overseeing the cybersecurity program, ensuring that appropriate responses are implemented during security incidents, and coordinating the incident response team. Cybersecurity management encompasses not just the immediate response to incidents but also the development of policies, strategies, and procedures to prevent these incidents from occurring in the first place. This role requires a comprehensive understanding of risk management, compliance, and the ongoing improvement of security measures within an organization. While other roles, such as a cybersecurity analyst, may focus on identifying and analyzing threats and vulnerabilities, they typically do not oversee the entire incident response process. Network administrators concentrate on maintaining and configuring network infrastructure, and technical support specialists assist users with specific technical issues but do not usually have a focused cybersecurity incident management role. Hence, the responsibilities of cybersecurity management are essential for effective incident handling and overall organizational security.

SAMPLE

7. What is the purpose of the recovery process after a security incident?

A. To improve documentation practices

B. To ensure business processes continue

C. To re-evaluate the budget

D. To conduct post-incident reviews

The recovery process following a security incident is primarily focused on ensuring that business processes continue functioning effectively. This phase is crucial because incidents can disrupt operations, lead to data loss, and affect overall business continuity. During recovery, organizations work to restore services and systems to normal operation as quickly and efficiently as possible, minimizing downtime and its associated impacts on productivity and revenue. While improving documentation practices, re-evaluating the budget, and conducting post-incident reviews may occur as part of a broader incident response or business continuity framework, the immediate priority during recovery is to bring affected business processes back online. The recovery efforts ensure that the organization can resume normal operations and maintain services to its stakeholders while addressing any vulnerabilities identified during the incident.

8. Which components are included in identity management?

A. Data processing techniques

B. Directory services and user management capabilities

C. Artificial intelligence algorithms

D. Physical security measures

Identity management is fundamentally about managing user identities and overseeing their access to various resources within an organization. This encompasses several important components, primarily directory services and user management capabilities. Directory services play a critical role in identity management as they provide the necessary infrastructure to store, retrieve, and manage user identity information in a centralized manner. They allow organizations to maintain records of user accounts, roles, and permissions, which facilitates efficient management of users within an IT environment. User management capabilities further enhance identity management by enabling administrators to create, modify, and delete user accounts; control access rights; and regulate authentication processes. This ensures that only authenticated and authorized individuals can access specific resources, thereby protecting sensitive information and maintaining overall security. In contrast, while data processing techniques, artificial intelligence algorithms, and physical security measures may be relevant to broader security or IT operations, they do not directly pertain to the core functions of identity management. Data processing techniques are focused more on handling and analyzing data rather than managing identities, AI algorithms may aid in security tasks but are not components of identity management itself, and physical security measures pertain to the protection of physical assets rather than user identity and access management. Thus, focusing on directory services and user management capabilities effectively encompasses the essential aspects of identity management

SAMPLE

9. What type of management focuses on maintaining the performance of a network?

A. Fault management

B. Accounting management

C. Performance management

D. Security management

Performance management is the area of network management dedicated to monitoring and optimizing the functioning of a network. It encompasses activities and processes aimed at ensuring that the network operates efficiently and effectively. This involves analyzing metrics such as bandwidth usage, latency, response times, and overall throughput to identify areas that require improvement or adjustment. By focusing on performance management, organizations can proactively address potential issues that may affect network speed and reliability, ensuring that users have a seamless experience when accessing network resources. The other areas of network management play distinct roles: fault management primarily deals with detecting and resolving network issues, accounting management focuses on tracking network resource usage for billing and auditing purposes, and security management is concerned with protecting the network from unauthorized access and threats. While each type of management is crucial for overall network health, performance management specifically targets the optimization and effectiveness of network operations.

10. In risk management, which of the following is a proactive approach?

A. Ignoring potential threats

B. Continuously evaluating emerging risks

C. Post-event analysis

D. Implementing last-minute fixes

In risk management, continuously evaluating emerging risks represents a proactive approach because it involves actively seeking to identify and assess potential threats before they materialize into significant issues. This ongoing assessment allows organizations to stay ahead of risks by adapting their strategies and controls to address these threats effectively. By focusing on identifying and understanding potential vulnerabilities prior to any incidents occurring, organizations can implement measures to mitigate the risks, thereby protecting their assets and ensuring continuity. In contrast, ignoring potential threats is a passive approach that leaves vulnerabilities unaddressed, while post-event analysis occurs after an incident has already taken place, making it more reactive than proactive. Implementing last-minute fixes also lacks a proactive stance, as it suggests a response to an imminent problem rather than a strategic assessment and management of risks beforehand. Thus, continuously evaluating emerging risks is essential for fostering a culture of preparedness and resilience in cybersecurity and risk management.

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://csxcybersecurityfund.examzify.com

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

SAMPLE