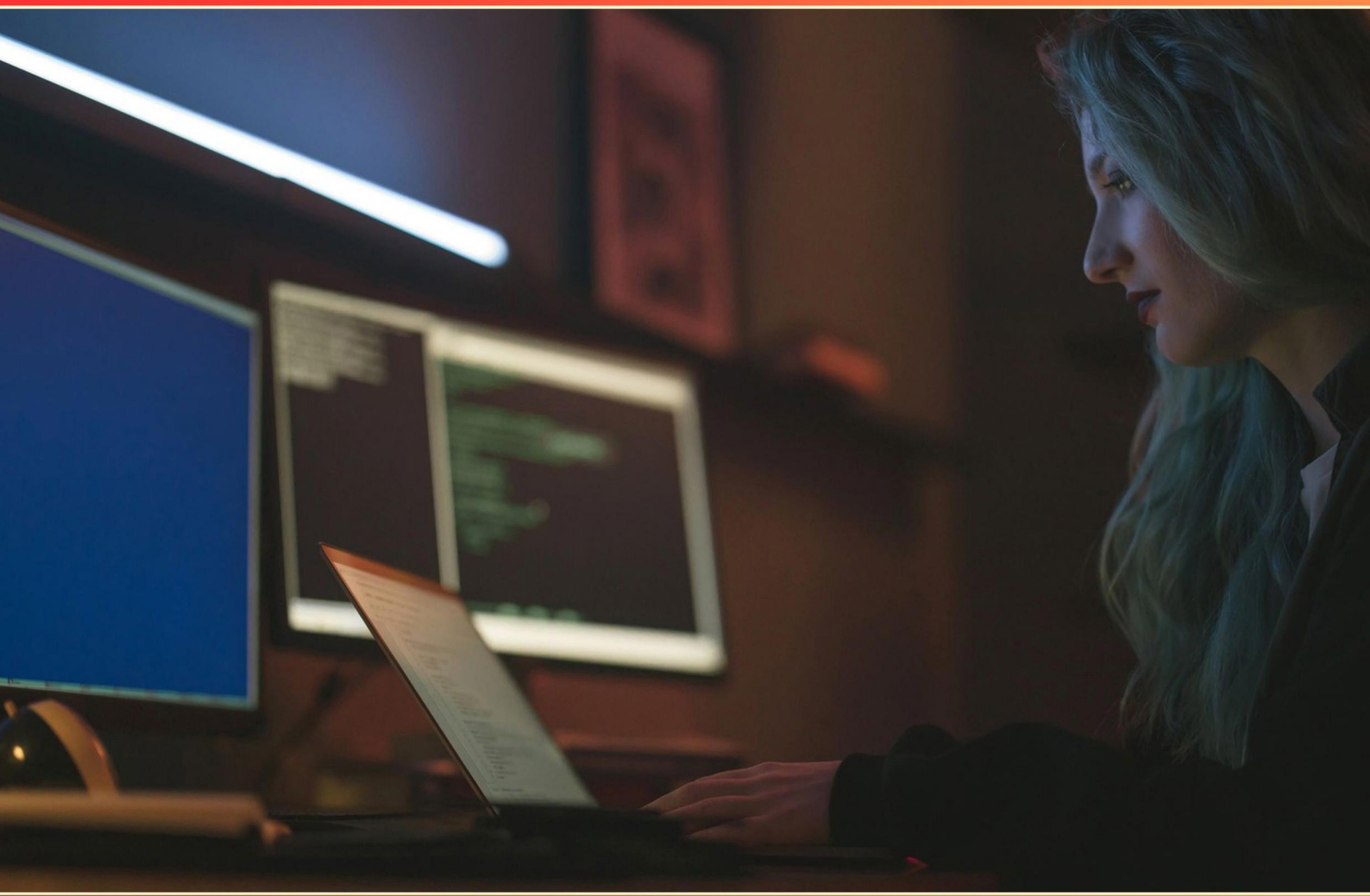
CYBER SECURITY CONNECT CONCEPTS PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cybersecconnectconcepts.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 NIST Cybersecurity Framework, which function addresses the correction of cybersecurity plans after a security event?**

   A. Recover (RC) function

   B. Protect (PR) function

   C. Identify (ID) function

   D. Respond (RS) function

2. **How does the probable maximum loss (PML) aid in cybersecurity?**

   A. It helps determine spending needed to adequately secure an organization's IT infrastructure

   B. It provides a fixed budget for security measures

   C. It eliminates the need for risk assessment

   D. It calculates the insurance premiums for businesses

3. **What is a security breach?**

   A. An event that enhances data protection

   B. Unauthorized access to data or networks

   C. A technique for improving user experience

   D. A software issue that requires updates

4. **What is used to enforce endpoint compliance with policies before granting network access?**

   A. Network Monitoring Systems

   B. Network Access Control

   C. Data Loss Prevention Systems

   D. Endpoint Detection and Response

5. **What is a characteristic of zero trust architecture?**

   A. Trust is granted by default

   B. Minimal verification is required for internal users

   C. Strict identity verification is enforced for all users

   D. Access is based solely on location

SAMPLE

6. What is the primary goal of patch management?

A. To enhance the aesthetic of software applications

B. To systematically manage updates for software applications and systems

C. To sell software licenses

D. To increase the number of software applications

7. Which of the following is prohibited by the Computer Fraud and Abuse Act?

A. Cyber blackmail

B. Intentionally destroying a computer

C. Accessing unauthorized data

D. All of the above

8. What is a firewall?

A. A software designed to create web applications

B. A network security device that monitors traffic

C. A type of malware that affects computer systems

D. A tool to assess network performance

9. Which NIST Cybersecurity Framework function emphasizes the protection of IT infrastructure?

A. Protect (PR) function

B. Respond (RS) function

C. Recover (RC) function

D. Identify (ID) function

10. Which of the following is NOT part of the Recover (RC) function in the NIST Cybersecurity Framework?

A. Improvements to cybersecurity plans

B. Incident detection

C. Communication with all stakeholders

D. System restoration

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. In the NIST Cybersecurity Framework, which function addresses the correction of cybersecurity plans after a security event?

A. Recover (RC) function

B. Protect (PR) function

C. Identify (ID) function

D. Respond (RS) function

The function in the NIST Cybersecurity Framework that addresses the correction of cybersecurity plans after a security event is the Recover function. This function focuses on establishing and maintaining plans for resilience and restoring any capabilities or services that were impaired due to a cybersecurity incident. After an event, the recovery phase is crucial for analyzing the incident, identifying lessons learned, and making necessary adjustments to improve future responses and readiness. The Recover function ensures that organizations can effectively restore operations and services and incorporate the knowledge gained from the incident into future risk management processes. This might involve updating response plans, enhancing safeguards, or improving preparedness measures to prevent similar incidents from occurring. In contrast, the Protect function focuses on implementing safeguards to ensure the delivery of critical services. The Identify function involves developing an understanding of the organization's risk management and cybersecurity posture. The Respond function includes the immediate actions taken during or after a cybersecurity incident to contain the event, mitigating its impact. While these functions play essential roles within the overall framework, the specific focus on correction and improvement post-incident aligns with the goals of the Recover function.

2. How does the probable maximum loss (PML) aid in cybersecurity?

A. It helps determine spending needed to adequately secure an organization's IT infrastructure

B. It provides a fixed budget for security measures

C. It eliminates the need for risk assessment

D. It calculates the insurance premiums for businesses

Probable Maximum Loss (PML) is a critical concept in risk management and cybersecurity, particularly in determining the extent of potential financial impact from cybersecurity incidents. By assessing PML, organizations can better understand the worst-case scenarios relating to their information security. This understanding directly informs their budgeting decisions regarding cybersecurity measures. When considering a PML analysis, organizations can gauge the maximum expected loss in the event of a significant security breach or incident. This helps them allocate resources effectively, ensuring that they invest in the right safeguards and technologies to protect their infrastructure. The findings from a PML assessment provide valuable insights that guide decision-makers in their security spending, enabling them to implement a robust cybersecurity posture that is commensurate with potential losses. The other options fail to encapsulate the true essence of PML. For instance, while the notion of building a fixed budget for security might sound applicable, it does not reflect the dynamic nature of cybersecurity expenses, which should adapt based on evolving risks and threats. Additionally, PML does not eliminate the necessity for risk assessments; rather, it can complement these assessments by giving a clearer picture of financial implications. Finally, while it is linked to financial aspects such as insurance premium calculations, the primary utility of PML lies more in guiding

SAMPLE

3. What is a security breach?

A. An event that enhances data protection

B. Unauthorized access to data or networks

C. A technique for improving user experience

D. A software issue that requires updates

A security breach is defined as unauthorized access to data or networks. This means that an individual or entity has gained access to information that should be protected, intentionally bypassing security protocols. Such breaches can lead to data theft, data corruption, or even loss of data integrity, often resulting in significant consequences for both individuals and organizations. Understanding this concept is crucial, as it highlights the vulnerabilities systems face and underscores the importance of implementing robust security measures to protect sensitive information. Unlike enhancements to data protection, user experience techniques, or software issues that can be resolved with updates, a security breach represents a critical failure of security measures, requiring immediate attention and remediation to prevent data exploitation.

4. What is used to enforce endpoint compliance with policies before granting network access?

A. Network Monitoring Systems

B. Network Access Control

C. Data Loss Prevention Systems

D. Endpoint Detection and Response

The correct choice, Network Access Control, plays a critical role in enforcing endpoint compliance with security policies prior to granting access to the network. This approach ensures that devices seeking to connect must meet specific criteria, which may include having up-to-date antivirus software, operating system patches, and other security measures in place. By verifying the security status of endpoints before they connect, Network Access Control helps to mitigate the risk of vulnerabilities being exploited by malicious actors. The other options do have their own roles within cybersecurity. Network Monitoring Systems focus on observing and analyzing network traffic to detect anomalies or potential threats but do not directly enforce compliance at the point of access. Data Loss Prevention Systems aim to prevent the unauthorized transfer of information but do not restrict network access based on endpoint security posture. Endpoint Detection and Response tools are designed to monitor and respond to threats on endpoints but do not serve the same purpose for pre-access compliance validation as Network Access Control does. Thus, the emphasis on enforcing compliance directly aligns with the role of Network Access Control.

SAMPLE

5. What is a characteristic of zero trust architecture?

A. Trust is granted by default

B. Minimal verification is required for internal users

C. Strict identity verification is enforced for all users

D. Access is based solely on location

A key characteristic of zero trust architecture is the enforcement of strict identity verification for all users, regardless of their location within or outside the network. This approach operates under the principle that no user or device should be trusted by default, even if they are within the organization's perimeter. In a zero trust model, continuous authentication and authorization are essential to verify user identities and ensure that they have the necessary permissions to access specific resources. This is particularly important in today's cybersecurity landscape, where threats can originate from both external and internal sources. By requiring strict identity verification of every user, every device, and every request, organizations can significantly reduce the risk of unauthorized access and potential data breaches. The zero trust philosophy emphasizes that security should be applied uniformly across all access attempts, effectively minimizing trust and enhancing protection. In contrast, options that imply granting trust by default, requiring minimal verification for internal users, or basing access solely on location do not align with zero trust principles, as they could introduce vulnerabilities by assuming inherent trust based on position or prior verification.

6. What is the primary goal of patch management?

A. To enhance the aesthetic of software applications

B. To systematically manage updates for software applications and systems

C. To sell software licenses

D. To increase the number of software applications

The primary goal of patch management is to systematically manage updates for software applications and systems. This process involves identifying, acquiring, testing, and installing patches to fix vulnerabilities or bugs in the software. By effectively implementing patch management, organizations can ensure that their systems are protected from known security threats, reduce the risk of exploits or attacks, and maintain compliance with regulatory requirements. Regular patch management is vital for maintaining the security and functionality of software, as unpatched systems can be especially vulnerable to various types of cyber threats. This approach not only addresses security issues but can also improve system performance and user experience by resolving bugs or issues present in the software. On the other hand, focusing on aesthetics, selling software licenses, or increasing the number of software applications does not address the critical need for maintaining software security and operational integrity that patch management fulfills.

SAMPLE

7. Which of the following is prohibited by the Computer Fraud and Abuse Act?

A. Cyber blackmail

B. Intentionally destroying a computer

C. Accessing unauthorized data

D. All of the above

The Computer Fraud and Abuse Act (CFAA) is a comprehensive piece of legislation aimed at addressing various forms of computer-related crime. It prohibits a range of unauthorized activities involving computers and data, protecting both the integrity of computer systems and the confidentiality of data. Cyber blackmail involves using threats to steal information or gain something of value, which is a fraudulent action addressed under the CFAA. Intentionally destroying a computer encompasses acts that damage computer systems, programs, or data, which the Act explicitly prohibits. Accessing unauthorized data involves entering computers or networks without permission to retrieve or manipulate data, which is a clear violation of the CFAA. By encompassing cyber blackmail, intentional destruction of computers, and unauthorized data access, the law aims to deter a wide array of cybercrimes that affect individuals and organizations. Therefore, all the mentioned activities fall under the prohibitions of the Computer Fraud and Abuse Act.

8. What is a firewall?

A. A software designed to create web applications

B. A network security device that monitors traffic

C. A type of malware that affects computer systems

D. A tool to assess network performance

A firewall is fundamentally a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its primary function is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet. By doing this, firewalls help protect networks from unauthorized access, cyberattacks, and various threats, ensuring that only legitimate traffic is allowed through. Firewalls can be either hardware-based, in the form of dedicated devices that filter data at the network level, or software-based, which typically run on individual computers and protect against threats at the operating system level. They can be configured to block or allow traffic based on specific criteria, such as IP addresses, domain names, protocols, and ports. In contrast, other choices like web application creation, malware, and network performance assessment do not align with the primary purpose of a firewall. They focus on different aspects of technology and security that are not directly related to the monitoring and control of network traffic, which is the core function of a firewall.

SAMPLE

9. Which NIST Cybersecurity Framework function emphasizes the protection of IT infrastructure?

A. Protect (PR) function

B. Respond (RS) function

C. Recover (RC) function

D. Identify (ID) function

The Protect (PR) function of the NIST Cybersecurity Framework is focused specifically on safeguarding critical infrastructure and information systems. This function emphasizes the implementation of appropriate safeguards to ensure the delivery of critical infrastructure services. It includes measures for access control, awareness and training, data security, maintenance, protective technology, and other relevant protections, all directed at preventing and mitigating cybersecurity risks. This function aims to mitigate the effects of potential cybersecurity-related events, ensuring that organizations can prevent or minimize the impact of a threat. By focusing on protective measures, organizations can create an environment that is resilient to attacks and capable of maintaining operations despite incidents, thereby securing their IT infrastructure from various threats. The other functions listed serve different purposes. The Respond (RS) function deals with developing and implementing appropriate activities to take action regarding a detected cybersecurity incident. The Recover (RC) function focuses on resilience and timely restoration of services after a cybersecurity event. The Identify (ID) function involves understanding the organizational environment and managing cybersecurity risks to systems, assets, data, and capabilities. While all these functions are crucial to a comprehensive cybersecurity strategy, only the Protect function specifically emphasizes the active protection of IT infrastructure.

10. Which of the following is NOT part of the Recover (RC) function in the NIST Cybersecurity Framework?

A. Improvements to cybersecurity plans

B. Incident detection

C. Communication with all stakeholders

D. System restoration

The Recover function in the NIST Cybersecurity Framework focuses on maintaining plans for resilience and restoring any capabilities or services that were impaired due to a cybersecurity incident. It includes activities involved in recovery planning, incident responses, and improvements after a security incident has occurred. Incident detection, which is the option identified, pertains more to the Detect function of the framework. Detecting incidents involves identifying cybersecurity events that may indicate a breach or vulnerability but does not fall under the processes involved in recovery. The Recover function, instead, emphasizes actions such as system restoration, improvements to cybersecurity plans based on lessons learned, and effective communication with all stakeholders involved in the recovery process. These components are vital for ensuring an organization can return to normal operations and strengthen its security posture against future incidents.

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://cybersecconnectconcepts.examzify.com

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

SAMPLE