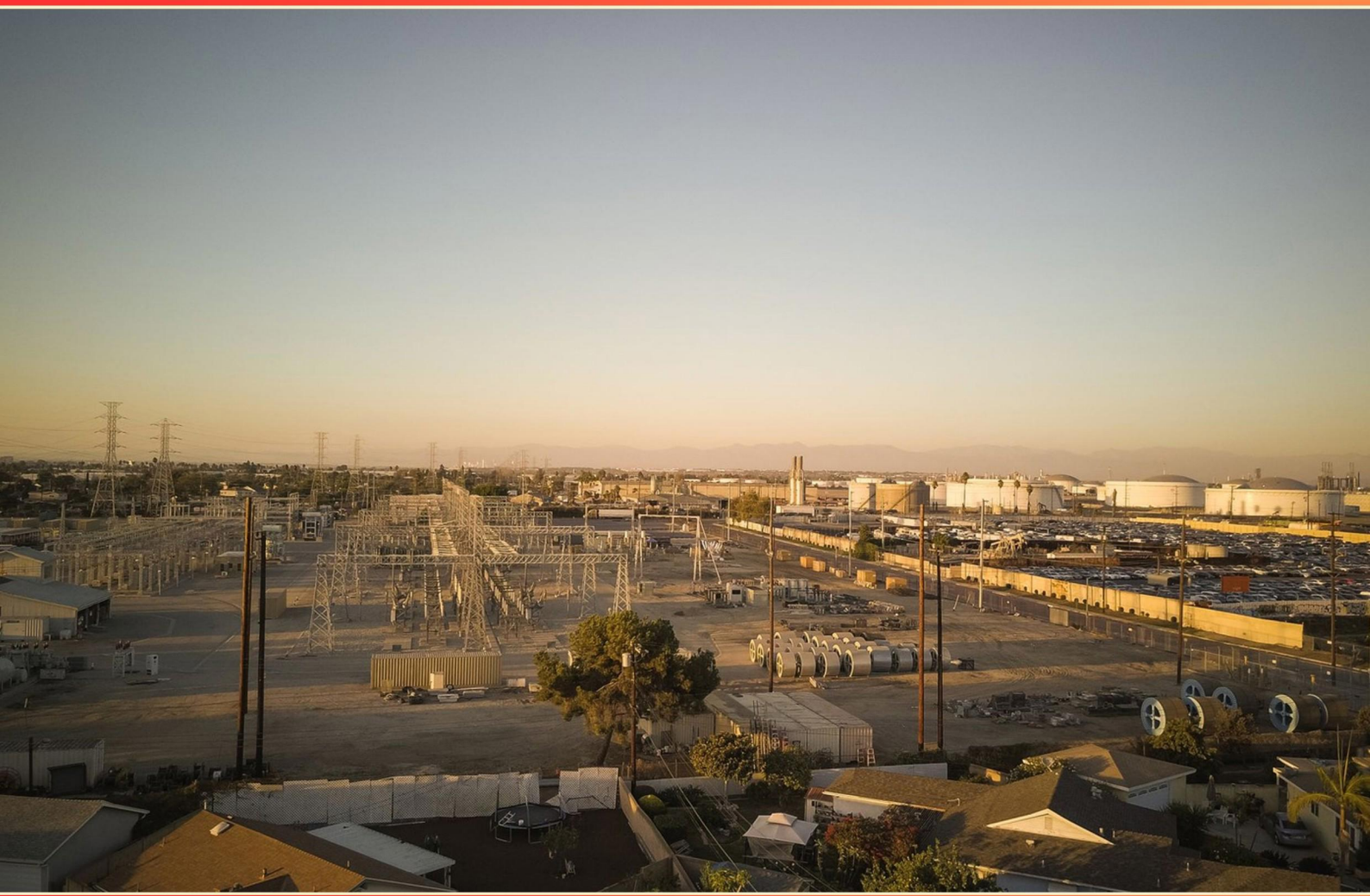
NERC CRITICAL INFRASTRUCTURE PROTECTION (CIP) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://nerccip.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 a firewall redundancy strategy, what defines a hot backup?

A. Requires manual configuration when activated

B. Instantly available for failover

C. Needs extensive testing before activation

D. Cannot handle traffic load

2. What is the initial notification timeframe for Reportable Cyber Security Incidents?

A. Within 12 hours

B. Within 24 hours

C. Within 1 hour

D. Within 2 hours

3. What is vital to consider in your patch management universe according to CIP-010?

A. A list of user roles

B. A security baseline inventory

C. A software license inventory

D. An asset depreciation schedule

4. How should unauthorized changes to the baseline configuration be handled?

A. Ignore them unless they are reported

B. Document and investigate the detected changes

C. Implement them if they enhance performance

D. Request feedback from users before acting

5. How often should logged events be reviewed, according to security event monitoring standards?

A. Every week

B. Every 15 calendar days

C. Every month

D. Once a quarter

SAMPLE

6. What are the primary components of the Four Legged Firewall?

A. Trusted, untrusted, DMZ for inbound traffic, DMZ for outbound traffic

B. External network, trusted network, isolated network segments, monitoring tools

C. Firewalls, intrusion detection systems, proxies, routers

D. Public network, private network, internet access, policy implementation

7. What should be done with the evidence collected for physical I/O ports?

A. Discard it after six months

B. Organize it for future audits

C. Share it only internally

D. Limit access to management only

8. What does Functional Registration require from entities?

A. To comply with financial regulations

B. To register for compliance with standards based on their functional responsibility

C. To participate in market operations

D. To submit annual financial reports

9. What distinguishes a scan of interest from a sequential port scan?

A. Sequential scans are faster and less predictable.

B. A scan of interest targets specific ICS ports.

C. Sequential scans do not reveal system vulnerabilities.

D. A scan of interest can only be performed from outside the network.

10. Which of the following describes a technical control for physical ports?

A. OS Policy Enforcement

B. Signage

C. Employee training

D. Disaster recovery plan

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. In a firewall redundancy strategy, what defines a hot backup?

A. Requires manual configuration when activated

B. Instantly available for failover

C. Needs extensive testing before activation

D. Cannot handle traffic load

A hot backup in a firewall redundancy strategy is one that is instantly available for failover. This means that in the case of a failure of the primary system, the hot backup can take over immediately without requiring any manual intervention or reconfiguration. The primary advantage of a hot backup is the minimization of downtime and the seamless continuity of service, which is crucial in environments where uptime is paramount. In contrast, a hot backup is specifically designed to stay active and synchronized with the primary unit, allowing for real-time failover. This immediacy is often achieved through constant monitoring and data replication processes, ensuring that the backup system is prepared to handle the same traffic load as the primary system at any moment. Other strategies, like a cold backup, would require significant configuration and manual steps to activate, making them less effective in situations where quick recovery is essential. Similarly, extensive testing before activation does not align with the 'hot' nature of this solution, as one would expect a hot backup to be fully tested and operational prior to reliance on it. Additionally, the capacity to handle traffic load is a fundamental aspect of a hot backup, and it is not accurate to say that it cannot manage this responsibility.

2. What is the initial notification timeframe for Reportable Cyber Security Incidents?

A. Within 12 hours

B. Within 24 hours

C. Within 1 hour

D. Within 2 hours

The correct initial notification timeframe for Reportable Cyber Security Incidents is one hour. This stringent requirement reflects the urgency and critical nature of cybersecurity threats in the context of critical infrastructure, ensuring that entities can quickly address potential risks. Timely notifications allow for an immediate assessment of the situation and facilitate coordinated responses, both internally and with relevant stakeholders or regulatory bodies. The one-hour requirement ensures that organizations prioritize incident reporting in alignment with NERC CIP standards, which are designed to safeguard the reliability of the grid and protect sensitive information from cyber threats. This rapid notification can be crucial in mitigating the impacts of a cyber incident and helps maintain the overall security posture of the affected organization.

SAMPLE

3. What is vital to consider in your patch management universe according to CIP-010?

A. A list of user roles

B. A security baseline inventory

C. A software license inventory

D. An asset depreciation schedule

Considering a security baseline inventory is crucial in the context of patch management as outlined by CIP-010. This standard focuses on maintaining the security of systems that are part of the critical infrastructure. A security baseline inventory provides a comprehensive list of all software and systems in use, and it establishes the minimum security requirements that need to be met. By having a clearly defined baseline, organizations are better equipped to identify which systems require updates or patches. This ensures that all vulnerabilities are addressed, and the systems remain in compliance with established security standards. This proactive approach helps maintain the integrity and availability of critical infrastructure components, as it allows for timely and efficient management of software vulnerabilities. The other options, while important in their own contexts, do not directly address the core requirements of patch management under CIP-010. User roles help define access rights but do not contribute to managing patches specifically. A software license inventory concerns the legality and compliance of software usage, while an asset depreciation schedule tracks the financial aspects of assets, neither of which are directly related to maintaining security through patch management.

4. How should unauthorized changes to the baseline configuration be handled?

A. Ignore them unless they are reported

B. Document and investigate the detected changes

C. Implement them if they enhance performance

D. Request feedback from users before acting

Handling unauthorized changes to the baseline configuration is crucial for maintaining the integrity and security of critical infrastructure systems. When there are changes that deviate from the established baseline configuration, it is essential to document and investigate these changes thoroughly. This process ensures that any potential security risks or vulnerabilities introduced by the unauthorized changes are identified and addressed. Documenting the unauthorized changes provides a record that can be reviewed later, which is important for compliance with NERC CIP standards. Investigating the changes allows personnel to understand the nature of the alterations and evaluate their impact on the system. This proactive approach is necessary to mitigate risks, ensure the system's reliability, and maintain compliance with regulatory standards. In contrast, ignoring the changes or implementing them without scrutiny can lead to security vulnerabilities, compliance failures, and potential operational disruptions. Requesting user feedback before acting may also delay necessary corrective actions and not provide the insight needed to address security concerns effectively. Such measures do not prioritize the critical assessment required to protect the infrastructure, making documentation and investigation the most prudent response.

SAMPLE

5. How often should logged events be reviewed, according to security event monitoring standards?

A. Every week

B. Every 15 calendar days

C. Every month

D. Once a quarter

The standard for reviewing logged events typically emphasizes the importance of timely and regular reviews to ensure that any security incidents can be promptly detected and responded to. Reviewing logged events every 15 calendar days aligns well with the guidelines put forth by NERC's Critical Infrastructure Protection (CIP) standards, which advocate for a detailed and frequent examination of security logs. This timeframe allows for a more effective monitoring process that helps to identify patterns or anomalies in security behavior before they escalate into serious threats. In the context of cybersecurity, more frequent reviews can lead to better situational awareness and rapid incident response, which are critical in protecting critical infrastructure. Longer intervals, such as monthly or quarterly reviews, could result in missed security incidents or delayed responses to potential threats, reducing an organization's ability to maintain its security posture effectively. Therefore, adhering to the 15-day review period is crucial for meeting the expectations set by regulatory standards and maintaining a robust security infrastructure.

6. What are the primary components of the Four Legged Firewall?

A. Trusted, untrusted, DMZ for inbound traffic, DMZ for outbound traffic

B. External network, trusted network, isolated network segments, monitoring tools

C. Firewalls, intrusion detection systems, proxies, routers

D. Public network, private network, internet access, policy implementation

The primary components of the Four Legged Firewall architecture are indeed centered around establishing a secure environment by creating distinct zones to manage and control traffic effectively. The model typically divides the network into four segments: a trusted network, an untrusted network, and two Demilitarized Zones (DMZs) for managing inbound and outbound traffic. In this framework, the trusted zone generally houses internal resources that are protected and require stringent access controls. The untrusted zone represents the external network, such as the internet, where threats can originate. The inbound DMZ serves as a buffer for incoming traffic to the trusted network, allowing for specific services to be accessed from external sources while still protecting internal resources. The outbound DMZ, on the other hand, is designed for managing outgoing traffic and ensuring that data leaving the trusted environment is screened and controlled. This structured approach helps mitigate risks by isolating different types of traffic and ensuring that only appropriate communications are allowed to pass between these zones. By having distinct boundaries, security policies can be implemented more effectively, focusing on specific traffic types and their associated risks. Thus, this setup enhances overall network security and compliance with frameworks like NERC's CIP requirements.

SAMPLE

7. What should be done with the evidence collected for physical I/O ports?

A. Discard it after six months

B. Organize it for future audits

C. Share it only internally

D. Limit access to management only

Organizing evidence collected for physical I/O ports for future audits is essential for maintaining compliance with NERC Critical Infrastructure Protection (CIP) standards. This practice ensures that any potential security incidents or audits can be effectively reviewed and analyzed later. Proper organization allows for easier access to evidence when needed, facilitating a structured response to any inquiries from regulators or internal audits regarding physical security measures. Maintaining thorough and organized records is crucial in demonstrating that an organization adheres to compliance requirements. It promotes accountability and provides a clear trail of the management of physical assets, all of which are vital components of a robust security posture. Other approaches, such as discarding evidence after a set timeframe or limiting access to just management, would not support effective compliance or risk management, as these could hinder the organization's ability to respond to incidents or audits effectively. Sharing internal records could lead to potential vulnerabilities if not managed properly, making organized retention the best practice.

8. What does Functional Registration require from entities?

A. To comply with financial regulations

B. To register for compliance with standards based on their functional responsibility

C. To participate in market operations

D. To submit annual financial reports

Functional Registration is a process specific to the NERC Critical Infrastructure Protection (CIP) that mandates entities to register based on their roles and responsibilities within the electrical grid system. This means that organizations must identify and register for compliance with specific reliability standards that apply to them, categorized by their functional responsibilities. For instance, different roles such as generator owners, transmission operators, and balancing authorities have distinct compliance requirements that correspond to their operational functions within the bulk power system. This registration process ensures that each entity is subject to the appropriate standards that govern their behavior and practices, ensuring consistent and effective management of reliability risks across the entire grid. By registering according to their functional responsibilities, entities can better align their operations with regulatory expectations, fostering overall grid reliability and security. In contrast, the other choices do not align with the specific focus of Functional Registration. Compliance with financial regulations or participation in market operations, while relevant to certain aspects of the energy sector, does not specifically address the core purpose of Functional Registration in the context of NERC standards. Submitting annual financial reports is also unrelated to the functional compliance requirements set forth by NERC, which are centered on operational roles and responsibilities rather than financial oversight.

SAMPLE

9. What distinguishes a scan of interest from a sequential port scan?

A. Sequential scans are faster and less predictable.

B. A scan of interest targets specific ICS ports.

C. Sequential scans do not reveal system vulnerabilities.

D. A scan of interest can only be performed from outside the network.

A scan of interest is specifically designed to target particular Industrial Control System (ICS) ports that are crucial for the integrity and security of the infrastructure. This focus allows organizations to concentrate their scanning efforts on the ports most relevant to their systems rather than performing a broad sweep that may cover less critical areas. By honing in on these key ports, a scan of interest can yield more actionable insights and help in identifying vulnerabilities or threats directly associated with the functionality of the ICS. In contrast, a sequential port scan generally involves scanning ports in a specific order, which may not necessarily target those most relevant to the specific security needs of ICS. Sequential scans can be less efficient as they may include a multitude of non-essential ports, leading to longer scan times without delivering targeted insights. The nature of sequential scans also means they can sometimes allow adversaries to predict the scan behavior and potentially evade detection or response. The other options touch on aspects of scanning practices but do not accurately represent the distinguishing features of a scan of interest compared to sequential scans. For instance, the specific targeting of essential ports sets a scan of interest apart, providing a strategic advantage in the monitoring and securing of critical infrastructure.

10. Which of the following describes a technical control for physical ports?

A. OS Policy Enforcement

B. Signage

C. Employee training

D. Disaster recovery plan

The correct answer emphasizes a specific method employed to secure physical ports, which are crucial access points to critical infrastructure. Technical controls focus on using technology and systematic approaches to regulate and monitor access. The choice related to OS Policy Enforcement refers to the implementation of policy-driven measures at the operating system level that ensure only authorized users and devices can access system resources. This is essential for maintaining the integrity and security of sensitive information and systems. In the context of physical ports, it implies that access is authenticated and controlled through established security protocols that are critical for safeguarding physical environments from unauthorized intrusion. Signage, while necessary for safety and awareness, does not offer a systematic or technological mechanism for protecting physical ports or managing access. It primarily serves an informational purpose rather than a control function. Employee training enhances awareness among staff regarding security practices and policies but does not serve as a direct technical control itself. This approach relies on human factors rather than automated or technological measures. A disaster recovery plan focuses on the strategies to restore operations after an incident and does not act as a proactive control for managing physical access to ports. Thus, OS Policy Enforcement stands out as the strongest technical control for ensuring the security of physical ports through systematic access regulation.

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://nerccip.examzify.com

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

SAMPLE