NERC Critical Infrastructure Protection (CIP) Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

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

Table of Contents

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.

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!

Questions

1. **What is a key focus of FERC Order 843?**
    - **A. Updating all Reliability Standards**
    - **B. Adding requirements for Low Impact assets**
    - **C. Retirement of older standards**
    - **D. Managing risks across all power generation types**

2. **What is one key consideration when applying patches?**
    - **A. Applying uniformly across all departments**
    - **B. Create a mitigation plan if patches cannot be applied**
    - **C. Limiting patches to only critical systems**
    - **D. Deferring updates until next quarter**

3. **What is an example of a facility type included in the bulk-power system under the Energy Policy Act of 2005?**
    - **A. Electric distribution systems**
    - **B. Bulk generation facilities**
    - **C. Control systems necessary for operating an interconnected network**
    - **D. Residential power systems**

4. **Which firewall type uses deep packet inspection to analyze content?**
    - **A. Stateless packet filtering firewall**
    - **B. Stateful inspection firewall**
    - **C. Application firewall**
    - **D. Redundant firewall**

5. **Which of the following is not one of the NERC Regional Entities?**
    - **A. Western Electric Coordinating Council**
    - **B. Northeast Power Coordinating Council**
    - **C. Energy Reliability Organization**
    - **D. Texas Reliability Entity**

6. **What should be done with the outputs from running configuration reviews?**
   - **A. Stored with no further action**
   - **B. Used as evidence of compliance**
   - **C. Deleted after review**
   - **D. Shared only with stakeholders**

7. **FERC Order 791 is primarily concerned with the changes resulting in which version of the CIP Standards?**
   - **A. Version 4**
   - **B. Version 5**
   - **C. Version 6**
   - **D. Version 7**

8. **How often should the identification of BES Cyber Assets be reviewed or updated?**
   - **A. Every 5 calendar months**
   - **B. At least every 15 months**
   - **C. Only during major system upgrades**
   - **D. Annually or as needed**

9. **Which process is critical for managing post-approval changes to the authorization scope?**
   - **A. Excluding user input after approval**
   - **B. Documenting and communicating approval details**
   - **C. Notifying users before changes are made**
   - **D. Ignoring the changes if they are minor**

10. **What clarification did FERC Order 706-B provide?**
    - **A. Nuclear facilities not regulated by the NRC are exempt from NERC CIP**
    - **B. All nuclear facilities must comply with NERC CIP**
    - **C. Cyber Security Standards only apply to BES assets**
    - **D. NERC must develop controls for all asset classes**

Answers

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

Explanations

1. What is a key focus of FERC Order 843?

A. Updating all Reliability Standards

B. Adding requirements for Low Impact assets

C. Retirement of older standards

D. Managing risks across all power generation types

The focus of FERC Order 843 is to enhance the security of Bulk Electric System (BES) by addressing low impact assets through new requirements. This order recognizes that even low impact assets can pose a risk to the overall reliability and cybersecurity of the power grid. By establishing specific protective measures and requirements for low impact assets, the order aims to ensure that all components of the BES are properly secured and contribute to maintaining the overall integrity of the system. This includes considerations for physical security measures, cyber security protocols, and compliance aspects that were previously less stringent for low impact assets. Other options, while relevant to the broader discussion of reliability standards and risk management, do not capture the specific intention of FERC Order 843. The order does not focus on updating all reliability standards comprehensively or retiring older standards but rather addresses the need for specific requirements related to low impact assets. Enhancing risk management across all power generation types is also important, but the primary intent of Order 843 is aligned more closely with the framework for low impact asset requirements.

2. What is one key consideration when applying patches?

A. Applying uniformly across all departments

B. Create a mitigation plan if patches cannot be applied

C. Limiting patches to only critical systems

D. Deferring updates until next quarter

When applying patches, creating a mitigation plan if patches cannot be applied is a crucial consideration. This practice ensures that organizations maintain a proactive stance toward security risks. If vulnerabilities are identified and patches cannot be immediately implemented—whether due to system compatibility issues, operational constraints, or other factors—having a mitigation plan in place allows the organization to address the potential risks in an alternative manner. This could involve implementing compensating controls, such as additional layers of security, enhanced monitoring, or limited access to the affected systems until the patch can be applied. It effectively reduces the window of exposure and helps maintain compliance with regulatory requirements, thus safeguarding critical infrastructure. The other choices may not adequately reflect the complexities and critical nature of effectively managing vulnerabilities through patches. For example, applying patches uniformly across all departments may not take into account the unique needs and risk profiles of different environments. Limiting patches to only critical systems may leave other vulnerable areas unprotected. Deferring updates can leave outdated systems exposed to threats for a prolonged period, which may violate best practices in risk management. Thus, having a well-thought-out mitigation plan offers flexibility and ensures comprehensive risk management when immediate patching isn't feasible.

3. What is an example of a facility type included in the bulk-power system under the Energy Policy Act of 2005?

A. Electric distribution systems

B. Bulk generation facilities

C. Control systems necessary for operating an interconnected network

D. Residential power systems

The correct answer highlights the vital role of control systems that are essential for the operation of an interconnected network, which is a core component of the bulk-power system as defined under the Energy Policy Act of 2005. These control systems manage the operation of various elements of the grid, ensuring stability, reliability, and efficiency in the delivery of electricity across the bulk power network. They facilitate coordination among different generation and transmission facilities, helping to respond to real-time changes in supply and demand, thus maintaining the integrity of the power system. Understanding this context underscores the importance of these control systems within the broader definition of the bulk-power system, as they enable the interconnected operation of different facilities and serve critical functions necessary for grid management and reliability. In contrast, while bulk generation facilities are significant, they are just one part of the interconnected infrastructure that includes both generation and transmission capabilities. Electric distribution systems and residential power systems fall outside the definition of the bulk-power system, which predominantly focuses on high-voltage transmission and generation capabilities essential for large-scale electricity delivery.

4. Which firewall type uses deep packet inspection to analyze content?

A. Stateless packet filtering firewall

B. Stateful inspection firewall

C. Application firewall

D. Redundant firewall

The application firewall is specifically designed to operate at the application layer of the OSI model, which allows it to understand and filter traffic based on the applications and services that generate the data. By performing deep packet inspection, this type of firewall is capable of analyzing the complete content of the data packets—not just their headers. This enables it to identify and block attacks based on the actual content being transmitted, rather than simply filtering out packets based on source or destination addresses. This capability is particularly important for identifying and mitigating application-level threats, such as SQL injection or cross-site scripting attacks, which are often hidden within the application data itself. Because application firewalls can interpret higher-level protocols, they provide an additional layer of security that goes beyond the capabilities of standard firewalls, which may not inspect the full data payload of packets. Understanding the role of an application firewall in this context highlights its importance in a comprehensive security strategy for protecting critical infrastructure.

5. Which of the following is not one of the NERC Regional Entities?

A. Western Electric Coordinating Council

B. Northeast Power Coordinating Council

C. Energy Reliability Organization

D. Texas Reliability Entity

The correct choice is based on the understanding of the structure and roles of the NERC (North American Electric Reliability Corporation) and its associated Regional Entities. The NERC is responsible for overseeing the reliability of the North American electrical grid, and it operates through several designated Regional Entities. The Western Electric Coordinating Council, Northeast Power Coordinating Council, and Texas Reliability Entity are all recognized as NERC Regional Entities that coordinate and enforce compliance with reliability standards within their respective regions. Each of these entities plays a vital role in ensuring that the electrical systems they oversee are reliable and operate efficiently. In contrast, the Energy Reliability Organization is not classified as a Regional Entity under NERC. Instead, it often refers to NERC itself in a broader context, emphasizing its role in overseeing and coordinating efforts to maintain reliability across the continent. Since the question specifically asks for an entity that is not a Regional Entity, the Energy Reliability Organization is the correct answer. Understanding the distinctions and specific roles of these organizations is crucial for recognizing the structure of electrical reliability governance in North America.

6. What should be done with the outputs from running configuration reviews?

A. Stored with no further action

B. Used as evidence of compliance

C. Deleted after review

D. Shared only with stakeholders

Using the outputs from running configuration reviews as evidence of compliance aligns with NERC CIP requirements, which emphasize the importance of thorough documentation and accountability in critical infrastructure protection. Configuration reviews are a vital part of ensuring that systems adhere to predetermined security policies and standards. By documenting the findings from these reviews, organizations create a traceable record that can be leveraged to demonstrate compliance with regulatory requirements during audits or inspections. This documentation not only offers proof of adherence to security practices but also helps in identifying areas for improvement and risk mitigation. In contrast, simply storing the outputs with no action taken or deleting them after review would undermine the purpose of conducting those reviews in the first place, as it would eliminate the opportunity for accountability and continuous improvement. Sharing outputs only with stakeholders may restrict the broader organizational learning that comes from analyzing and acting on the findings collectively. Utilizing the outputs as evidence of compliance supports a culture of transparency and due diligence, which is essential for maintaining robust security postures in critical infrastructure.

7. FERC Order 791 is primarily concerned with the changes resulting in which version of the CIP Standards?

A. Version 4

B. Version 5

C. Version 6

D. Version 7

FERC Order 791 specifically addresses the revisions that resulted in the implementation of Version 5 of the NERC Critical Infrastructure Protection (CIP) Standards. This order was significant as it approved the changes made in Version 5, which introduced a variety of new requirements aimed at strengthening the security posture of the electric grid against cyber threats. Notably, these revisions focused on enhancing security measures surrounding the critical cyber assets, including aspects such as risk assessment and the protection of information systems. While later versions, such as Version 6 and Version 7, have made further updates and refinements, Order 791 is particularly linked to the transition to Version 5, making it pivotal in the history of the NERC CIP standards journey. This context is essential to understand the evolution of cybersecurity frameworks within the electric sector and how regulatory measures like FERC orders shape these standards over time.

8. How often should the identification of BES Cyber Assets be reviewed or updated?

A. Every 5 calendar months

B. At least every 15 months

C. Only during major system upgrades

D. Annually or as needed

The identification of Bulk Electric System (BES) Cyber Assets should be reviewed or updated at least every 15 months to ensure compliance with NERC Critical Infrastructure Protection (CIP) standards. This interval allows organizations to stay current with any changes in their assets that could impact security or operational integrity. By doing this regularly, organizations can identify and manage any new or altered assets that may arise due to changes in technology, system modifications, or new vulnerabilities that could be exploited. Regularly reviewing and updating the identification of BES Cyber Assets is essential for maintaining a strong security posture, as it ensures that all critical components are accounted for and properly safeguarded against threats. This proactive approach helps in effective risk management, as it allows for timely updates to security measures and practices aligned with an evolving threat landscape. The specified time frame, which is at least 15 months, ensures that organizations are not falling too far behind in their assessments, while also providing a structured timeline that can lead to more effective overall management of cyber assets.

9. Which process is critical for managing post-approval changes to the authorization scope?

A. Excluding user input after approval

B. Documenting and communicating approval details

C. Notifying users before changes are made

D. Ignoring the changes if they are minor

The process of documenting and communicating approval details is essential for managing post-approval changes to the authorization scope because it ensures that all stakeholders are aware of the established boundaries and any modifications to those boundaries. This practice enhances transparency and accountability, enabling effective monitoring of compliance with established security policies. When changes are thoroughly documented and communicated, it minimizes the risks of misunderstandings or unauthorized actions that could jeopardize the security of critical infrastructure. By successfully documenting and communicating the approval details, an organization can track changes made, the reasoning behind those changes, and maintain a clear record for auditing purposes. This is particularly important in environments governed by regulations like those outlined by NERC, where oversight and adherence to security protocols are critical for maintaining the integrity of critical infrastructure. This process also supports collaboration and information sharing among various teams, ensuring that security measures remain robust even in the face of necessary adjustments to the authorization scope.

10. What clarification did FERC Order 706-B provide?

A. Nuclear facilities not regulated by the NRC are exempt from NERC CIP

B. All nuclear facilities must comply with NERC CIP

C. Cyber Security Standards only apply to BES assets

D. NERC must develop controls for all asset classes

FERC Order 706-B clarified that all nuclear facilities, regardless of their regulatory status with the Nuclear Regulatory Commission (NRC), are required to comply with the NERC Critical Infrastructure Protection (CIP) standards. This directive ensured a uniform security framework across all nuclear facilities, emphasizing the importance of maintaining robust cybersecurity measures in protecting critical energy infrastructure. The inclusion of all nuclear facilities under NERC CIP reflects the recognition of their critical role in the electric grid and the necessity for stringent cybersecurity practices to mitigate risks associated with cyber threats. By mandating compliance across the board, FERC aimed to enhance overall grid reliability and security, ensuring that all potential vulnerabilities in the nuclear sector are addressed. The other options do not align with the intent or content of FERC Order 706-B. For instance, while some facilities may fall under various regulatory bodies, the emphasis here was on uniform compliance rather than exemptions or specific asset classifications. As such, the order represented a proactive measure in fortifying cybersecurity across the essential infrastructure tied to energy production and distribution.

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!