Federal IT Security Professional (FITSP) Auditor 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 one of the requirements of the Clinger-Cohen Act for federal agencies?**

   A. To enhance public access to federal information

   B. To conduct regular evaluations of IT systems

   C. To adopt a broad range of information technology

   D. To have a structured system acquisition strategy

2. **What is a key focus of the FedRAMP program?**

   A. Standardizing user access across systems

   B. Promoting continuous monitoring of security controls

   C. Streamlining the authorization process for cloud services

   D. Enhancing physical security at all agency facilities

3. **What is the correct order of the four components of risk management?**

   A. Monitor, Frame, Respond, Assess

   B. Frame, Assess, Respond, Monitor

   C. Frame, Assess, Monitor, Respond

   D. Frame, Assess, Respond, Monitor

4. **What is the purpose of common controls in an organization?**

   A. To enforce policy compliance

   B. To reduce redundancy across systems

   C. To increase system performance

   D. To eliminate the need for individual controls

5. **Which SCAP specification provides a standard naming convention for operating systems, hardware, and applications?**

   A. CVE

   B. CCE

   C. CWE

   D. CPE

6. A hard drive pulled from an unclassified information system containing high confidentiality information will be reused. What is the recommended course of media sanitization?

A. Clear

B. Purge

C. Degauss

D. Destroy

7. What are the four components of the new Risk Management Model?

A. Frame Risk, Allocate Risk, Respond to Risk, Monitor Risk

B. Frame Risk, Assess Risk, Prepare for Risk, Monitor Risk

C. Frame Risk, Assess Risk, Respond to Risk, Monitor Risk

D. Identify Risk, Assess Risk, Respond to Risk, Monitor Risk

8. Which SCAP specifications provide a standard naming convention for operating systems, hardware, and applications?

A. Common Platform Enumeration (CPE)

B. Common Vulnerability Enumeration (CVE)

C. Common Configuration Enumeration (CCE)

D. Common Weakness Enumeration (CWE)

9. What does SSP refer to after a risk assessment?

A. Security Strategy Plan

B. System Security Plan

C. Security Solutions Profile

D. Systems Support Plan

10. Which of the following is NOT a type of security control?

A. System-specific

B. Hybrid

C. Derived

D. Common

Answers

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

Explanations

1. What is one of the requirements of the Clinger-Cohen Act for federal agencies?

A. To enhance public access to federal information

B. To conduct regular evaluations of IT systems

C. To adopt a broad range of information technology

D. To have a structured system acquisition strategy

The Clinger-Cohen Act, enacted in 1996, emphasizes the need for federal agencies to establish a structured approach to managing information technology resources. One of the key requirements of the Act is to have a comprehensive system acquisition strategy. This is critical because it ensures that agencies develop and maintain an effective and efficient procurement process for IT systems, aligning their IT investments with their overall mission and performance goals. A structured system acquisition strategy involves processes for planning, acquiring, and managing IT resources, which can significantly enhance the effectiveness of technology solutions within government agencies. This approach helps minimize waste and redundancy while encouraging the adoption of best practices in IT governance. It fosters accountability and transparency, leading to better outcomes for the use of federal resources. While the other options may touch on important aspects of IT management or policy, they do not specifically capture the structured acquisition emphasis that the Clinger-Cohen Act mandates. The Act focuses on improving the acquisition and management processes rather than solely enhancing public access, conducting evaluations, or adopting a broad range of technologies without a strategy.

2. What is a key focus of the FedRAMP program?

A. Standardizing user access across systems

B. Promoting continuous monitoring of security controls

C. Streamlining the authorization process for cloud services

D. Enhancing physical security at all agency facilities

The FedRAMP program, or the Federal Risk and Authorization Management Program, is primarily aimed at providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud services used by federal agencies. The focus on streamlining the authorization process for cloud services allows agencies to expedite the acquisition of cloud solutions while ensuring that these services meet rigorous security standards. By establishing a standardized process, FedRAMP reduces the redundancy of individual assessments and allows multiple agencies to leverage a single security assessment of cloud services. This not only accelerates the time-to-market for cloud solutions but also ensures that the services provided are vetted for security compliance against the established federal standards. While continuous monitoring of security controls is an important component of the overall strategy of FedRAMP, the primary aim is indeed to improve the efficiency and effectiveness of the authorization process which agencies must navigate to deploy cloud services securely. This results in a more cohesive and secure cloud service environment for federal data and operations.

3. What is the correct order of the four components of risk management?

A. Monitor, Frame, Respond, Assess

B. Frame, Assess, Respond, Monitor

C. Frame, Assess, Monitor, Respond

D. Frame, Assess, Respond, Monitor

The correct order of the four components of risk management is essential for establishing a structured approach to identifying, evaluating, and addressing risks in an organization. Starting with "Frame," this first step involves defining the context of the risk management process, including understanding the organization's mission, objectives, and the risk tolerance level. This foundational component sets the stage for the subsequent steps by highlighting what is at stake and the criteria for evaluating potential risks. Next is "Assess," where the organization identifies and evaluates risks to determine their likelihood and potential impact. This step often includes identifying vulnerabilities, understanding threats, and prioritizing risks based on their potential consequences. A thorough assessment helps to paint a clearer picture of the organization's risk landscape. Following assessment is "Respond." In this stage, the organization develops strategies to address identified risks. This could involve implementing measures to mitigate risks, transferring the risk, accepting it, or avoiding it altogether. The effectiveness of the response depends on the insights gained during the assessment phase. Finally, "Monitor" is the last component, where ongoing observation of the risk environment and the effectiveness of risk management strategies occurs. Continuous monitoring ensures that the organization can adapt to changes in risks or should any previously settled risks evolve. This sequence— framing, assessing,

4. What is the purpose of common controls in an organization?

A. To enforce policy compliance

B. To reduce redundancy across systems

C. To increase system performance

D. To eliminate the need for individual controls

The purpose of common controls in an organization primarily revolves around the concept of managing security controls that can be applied across multiple systems or services. By utilizing common controls, organizations can effectively reduce redundancy across systems. This means that rather than implementing separate controls for every individual system, organizations can implement a single control that applies to multiple systems, streamlining security efforts and reducing the complexity of management. This approach not only saves time and resources but also enhances the consistency of security measures across different systems. Common controls can cover various functionalities, such as access control management, incident response procedures, and data protection measures. By centralizing these controls, organizations improve their efficiency and make it easier to maintain compliance with security policies and regulations, as well as facilitate audits and assessments. The other options highlight important considerations in information security but do not capture the primary purpose of common controls as effectively. For instance, while enforcing policy compliance is indeed vital, it is more of a result of having effective common controls rather than their purpose. Similarly, enhancing system performance is typically a secondary effect rather than a direct objective of common controls. Finally, while common controls can significantly reduce the need for individual controls, they do not completely eliminate the necessity for specific controls in certain scenarios where specialized measures are warranted.

5. Which SCAP specification provides a standard naming convention for operating systems, hardware, and applications?

A. CVE

B. CCE

C. CWE

D. CPE

The correct answer is the specification that provides a standard naming convention for operating systems, hardware, and applications, which is known as CPE (Common Platform Enumeration). CPE is a structured naming scheme that allows for the identification of specific hardware and software products. It utilizes a standardized format to create names that are machine-readable, facilitating interoperability among different security tools and organizations. This is particularly helpful for managing vulnerabilities and compliance across different platforms because it ensures that there is a consistent way to reference various software and hardware assets. The adherence to a standard naming convention supports better communication and data exchange among information security systems. In contrast, the other options serve different purposes within the realm of cybersecurity. CVE (Common Vulnerabilities and Exposures) provides a list of publicly known cybersecurity vulnerabilities; CCE (Common Configuration Enumeration) deals with identifying and naming configuration issues; and CWE (Common Weakness Enumeration) focuses on defining software weaknesses and vulnerabilities. Each of these plays a crucial role in the broader context of security management, but they do not specifically address the naming conventions for operating systems, hardware, and applications like CPE does.

6. A hard drive pulled from an unclassified information system containing high confidentiality information will be reused. What is the recommended course of media sanitization?

A. Clear

B. Purge

C. Degauss

D. Destroy

The recommended course of media sanitization in this scenario is to purge the hard drive. Purging involves using methods that render the data unrecoverable but still allow for the media to be reused or repurposed. This is particularly relevant when dealing with hard drives that have contained high confidentiality information, as purging typically includes techniques such as overwriting the data multiple times, which is effective at preventing unauthorized recovery of sensitive information. In the context of hard drive reuse, purging provides a balance between ensuring that sensitive data cannot be accessed and maintaining the usability of the hard drive for future applications. This aligns with federal standards that govern the sanitization of media containing sensitive information, highlighting the importance of confidentiality while also considering practicality in reuse. Other options, while useful in certain contexts, do not suit the requirements for a hard drive meant for reuse. Clearing data, for example, makes it difficult but not impossible to recover, which would not suffice for high confidentiality information. Degaussing is effective for magnetic media but renders the drive unusable afterward. Destroying the hard drive is the most extreme form of sanitization, ensuring data is completely unrecoverable but negating any possibility of future use. Therefore, purging best meets the needs of secure data sanit

7. What are the four components of the new Risk Management Model?

A. Frame Risk, Allocate Risk, Respond to Risk, Monitor Risk

B. Frame Risk, Assess Risk, Prepare for Risk, Monitor Risk

C. Frame Risk, Assess Risk, Respond to Risk, Monitor Risk

D. Identify Risk, Assess Risk, Respond to Risk, Monitor Risk

The four components of the new Risk Management Model focus on the systematic process for managing risks effectively. The components outlined in the correct answer—Frame Risk, Assess Risk, Respond to Risk, and Monitor Risk—provide a comprehensive approach to understanding and addressing risk within an organization. "Frame Risk" involves establishing the context for risk management, which includes defining the objectives, identifying stakeholders, and determining the risk criteria that will guide the risk management process. This important initial step sets the foundation for managing risks by ensuring that everyone involved understands the parameters and scope of the risk management effort. "Assess Risk" is the phase where risks are identified and analyzed to understand their potential impact on the organization. This includes evaluating the likelihood of risks occurring and the potential consequences, allowing the organization to prioritize risks based on their severity. "Respond to Risk" involves determining appropriate strategies to mitigate or address identified risks. This may include accepting, transferring, avoiding, or reducing risks through various controls and measures tailored to fit the organization's risk tolerance and operational context. Finally, "Monitor Risk" is critical for tracking the effectiveness of risk management strategies and ensuring that the organization remains adaptable to changes in the risk landscape. Through continuous monitoring, organizations can adjust their risk responses and improve their overall risk management

8. Which SCAP specifications provide a standard naming convention for operating systems, hardware, and applications?

A. Common Platform Enumeration (CPE)

B. Common Vulnerability Enumeration (CVE)

C. Common Configuration Enumeration (CCE)

D. Common Weakness Enumeration (CWE)

The choice of the Common Platform Enumeration (CPE) as the correct answer is rooted in its purpose and function within the context of security compliance and vulnerability management. CPE provides a standardized way to identify and name operating systems, hardware, and applications. This standardization is important because it enables consistent communication and reporting across different platforms and tools. It helps ensure that security software and tools can accurately identify the products and technologies that are in use, facilitating more effective assessments in both compliance and vulnerability management activities. By using a structured naming convention, CPE allows organizations to manage and reference their assets more effectively, which is particularly useful in the context of vulnerability analysis and security assessments. This standardization is critical for conducting thorough security assessments and keeping up with the current state of vulnerabilities associated with the specific platforms in use. In contrast, other options focus on different aspects of security metrics and standards. The Common Vulnerability Enumeration (CVE) identifies vulnerabilities, while the Common Configuration Enumeration (CCE) deals with specific configurations, and the Common Weakness Enumeration (CWE) addresses software weaknesses. None of these options serve the role of establishing a standardized naming convention for operating systems, hardware, and applications as effectively as CPE does.

9. What does SSP refer to after a risk assessment?

A. Security Strategy Plan

B. System Security Plan

C. Security Solutions Profile

D. Systems Support Plan

The designation "SSP" stands for System Security Plan. After conducting a risk assessment, an organization develops a System Security Plan as part of its efforts to document the security controls that are in place, as well as outline the measures necessary to protect the system and its data. This plan serves as a comprehensive description of the security requirements of the system, provides guidelines for how security measures will be implemented and provides a basis for ongoing security assessments.   The System Security Plan is essential for compliance with various regulatory and framework requirements such as NIST SP 800-53, which outlines controls that organizations need to meet to safeguard information systems. By articulating the security posture and addressing potential risks identified in the risk assessment, the SSP helps to ensure that appropriate resources are allocated and that security practices are consistently applied throughout the lifecycle of the system.

10. Which of the following is NOT a type of security control?

A. System-specific

B. Hybrid

C. Derived

D. Common

The identification of "derived" as the option that is not a type of security control reflects an understanding of the classifications of security controls in the context of information security.   Security controls are generally categorized into specific types to help organizations establish effective security measures. System-specific controls are tailored to particular systems and their unique risks. Common controls apply universally across multiple systems and are often part of an organization's broader IT infrastructure. Hybrid controls combine elements of both system-specific and common controls, used for special cases where a singular approach may not address security needs adequately. The term "derived," however, is not a recognized category of security controls within the established frameworks of security management. Instead, it may refer to the process of generating additional controls based on existing ones, rather than being a standalone category that can be classified similarly to the other types listed. Understanding the definitions and applications of various security control types is essential for anyone involved in auditing or managing information systems, as it helps in selecting and implementing appropriate measures to mitigate risks.

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://fitspauditor.examzify.com

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