FEDERAL IT SECURITY PROFESSIONAL (FITSP) AUDITOR PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://fitspauditor.examzify.com

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 control emphasizes the significance of the security categorization process?**

   A. PM-10 Security Authorization Process

   B. PM-11 Mission/Business Process Definition

   C. CA-6 Security Authorization

   D. PL-2 System Security Plan

2. **Which of the following is NOT a requirement under the OMB memo M-06-16?**

   A. Data encryption on mobile devices

   B. Regular audits of data access

   C. Two-factor authentication for remote access

   D. Timeout functions for inactive devices

3. **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)

4. **Which security mechanism is specifically designed to ensure that a message is not altered in transit?**

   A. Encryption

   B. Digital Signature

   C. Checksum

   D. Message Integrity Check

5. **What is the correct order of the Risk Management Framework process?**

   A. Categorize, Select, Implement, Assess, Authorize, Monitor

   B. Assess, Categorize, Select, Implement, Authorize, Monitor

   C. Assess, Categorize, Authorize, Select, Implement, Monitor

   D. Select, Assess, Categorize, Authorize, Implement, Monitor

6. What are the two most important factors when selecting a security control assessor?

A. Independence/Expertise

B. Trustworthiness/Experience

C. Expertise/Trustworthiness

D. Experience/Independence

7. Which special publication provides guidelines on designing, developing, conducting, and evaluating test, training, and exercise events?

A. NIST SP 800-53

B. NIST SP 800-84

C. NIST SP 800-37

D. NIST SP 800-18

8. What establishes the scope of protection for organizational information systems?

A. Net-centered Architecture

B. Dynamic External Subsystems

C. System Boundaries

D. System Security Plan

9. Which act outlines guidelines specifically for agency-wide security programs in federal agencies?

A. E-Government Act of 2002

B. Federal Information Security Management Act (FISMA)

C. Privacy Act, 1974

D. Government Information Security Reform Act (GISRA)

10. What form of cryptographic service is used to establish non-repudiation?

A. Symmetric Key Encryption

B. Digital Signature

C. Message Digest

D. Hashing Algorithm

Answers

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

Explanations

1. What control emphasizes the significance of the security categorization process?

A. PM-10 Security Authorization Process

B. PM-11 Mission/Business Process Definition

C. CA-6 Security Authorization

D. PL-2 System Security Plan

The control that emphasizes the significance of the security categorization process is PM-11 Mission/Business Process Definition. This control is foundational in aligning security measures with the critical missions and business functions of an organization. It ensures that a comprehensive understanding of the organization's mission and business processes informs the security categorization of the information systems involved. By recognizing the importance of categorization, PM-11 facilitates a structured approach to identifying the impact levels of potential security breaches based on the organization's operational needs. This reflects the necessity of tailoring security controls to the specific context of the mission or business objectives, ensuring that security efforts are prioritized effectively. This choice emphasizes that security is not an isolated aspect but is integral to the operation of business processes. For agencies operating under federal guidelines, this means that every system's security should be documented and justified based on its role within the mission framework, facilitating informed decision-making regarding risk management and resource allocation. Understanding this control helps auditors recognize how security categorization can affect overall risk management and ensure compliance with federal standards.

2. Which of the following is NOT a requirement under the OMB memo M-06-16?

A. Data encryption on mobile devices

B. Regular audits of data access

C. Two-factor authentication for remote access

D. Timeout functions for inactive devices

The correct understanding of the requirements under OMB memo M-06-16 highlights that one of the specific mandates does not pertain to regular audits of data access, making that option not a requirement of the memo. OMB memo M-06-16 emphasizes the protection of sensitive information in mobile devices, advocating for robust measures such as data encryption, two-factor authentication for enhancing remote access security, and timeout functions for inactive devices to prevent unauthorized access. These requirements are vital for ensuring the integrity and confidentiality of data, especially given the risks associated with mobile technology and remote access. While regular auditing is an essential practice in information security, it is not explicitly outlined in this particular memo as a mandated requirement. The focus of the memo is more on implementing specific protective measures rather than the auditing of data access itself. Thus, highlighting the elements that enhance security on mobile platforms and their access is the primary context of OMB M-06-16.

3. 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.

4. Which security mechanism is specifically designed to ensure that a message is not altered in transit?

A. Encryption

B. Digital Signature

C. Checksum

D. Message Integrity Check

The correct choice is based on the fundamental purpose of a digital signature, which is to provide assurance that a message has not been altered during transmission. A digital signature uses cryptographic techniques to create a unique fingerprint of a message. When a sender signs a document with their private key, a recipient can verify the signature with the sender's public key, ensuring the integrity and authenticity of the message. This verification process is crucial because it not only confirms that the message originated from the purported sender (authenticity) but also checks if the content of the message has remained unchanged since it was signed, thereby ensuring that any unauthorized alterations are detectable. While other choices relate to different aspects of security, they do not specifically address the dual purpose of ensuring message integrity and authenticity. For instance, encryption primarily focuses on confidentiality, ensuring that only authorized parties can read the message, but it doesn't provide a means to verify whether the message was altered. Similarly, checksums and message integrity checks are used to detect changes in data but do not provide the same level of assurance regarding the identity of the sender and the authenticity of the message as a digital signature does.

5. What is the correct order of the Risk Management Framework process?

A. Categorize, Select, Implement, Assess, Authorize, Monitor

B. Assess, Categorize, Select, Implement, Authorize, Monitor

C. Assess, Categorize, Authorize, Select, Implement, Monitor

D. Select, Assess, Categorize, Authorize, Implement, Monitor

The correct order of the Risk Management Framework (RMF) process is indeed to categorize, select, implement, assess, authorize, and monitor. This sequence is crucial because each step builds on the previous one, ensuring a comprehensive approach to managing risks associated with information systems. Starting with categorization is essential as it establishes the security requirements based on the impact levels of the information types handled by the system. This initial step informs decisions in the subsequent phases. After categorization, selecting the appropriate security controls comes next to ensure that the protections align with the system's identified risks. The implementation phase follows, where the selected controls are put into place within the system. This action needs to be thoroughly documented as part of the assessment phase, during which the effectiveness of the controls is evaluated against the defined security requirements. Once assessment is complete, the authorization process allows designated officials to review the system's risk posture and accept the risk prior to going live. Finally, continuous monitoring ensures that the system remains compliant and effective against evolving threats and vulnerabilities over time. Understanding this sequential process highlights how critical each step is in creating a robust risk management strategy in accordance with federal standards.

6. What are the two most important factors when selecting a security control assessor?

A. Independence/Expertise

B. Trustworthiness/Experience

C. Expertise/Trustworthiness

D. Experience/Independence

Selecting a security control assessor is critical for ensuring the effectiveness and integrity of an organization's security posture. Independence and expertise stand out as the two most important factors in this selection process. Independence is crucial because it ensures that the assessment is unbiased. An independent assessor can provide an objective evaluation without any conflicts of interest that might arise if they were closely tied to the organization's operations or security team. This objectivity is vital for fostering trust in the assessment's findings and recommendations, allowing for a transparent evaluation of the security controls in place. Expertise is equally important, as a competent security control assessor must possess extensive knowledge and experience in evaluating security frameworks, compliance requirements, and best practices. Their expertise enables them to identify vulnerabilities and weaknesses effectively, ensuring that all relevant aspects of the security controls are scrutinized thoroughly. This proficiency also means they can offer valuable insights and recommendations based on industry standards and past experiences. Together, independence and expertise create a strong foundation for a security control assessment, leading to actionable insights and improvements in an organization's security posture.

7. Which special publication provides guidelines on designing, developing, conducting, and evaluating test, training, and exercise events?

A. NIST SP 800-53

B. NIST SP 800-84

C. NIST SP 800-37

D. NIST SP 800-18

The choice of NIST SP 800-84 is correct because this special publication specifically addresses guidelines for designing, developing, conducting, and evaluating test, training, and exercise events related to information security. It is focused on helping organizations build effective and efficient testing and training programs, ensuring that personnel are adequately prepared to respond to security incidents and understand their roles within an organization's cybersecurity framework. By providing structured methodologies for such activities, NIST SP 800-84 emphasizes the importance of continuous improvement in security preparedness and the validation of security controls through practical exercises. This ensures that organizations can assess their security posture, identify gaps, and enhance their incident response capabilities based on documented best practices. In contrast, NIST SP 800-53 focuses on security and privacy controls for federal information systems and organizations, while NIST SP 800-37 deals with the Risk Management Framework. NIST SP 800-18 outlines the security and privacy planning for federal information systems. These publications serve different purposes and contexts, underscoring why SP 800-84 is uniquely positioned to provide the specific guidelines requested in the question.

8. What establishes the scope of protection for organizational information systems?

A. Net-centered Architecture

B. Dynamic External Subsystems

C. System Boundaries

D. System Security Plan

The correct answer is the designation of system boundaries, which establishes the scope of protection for organizational information systems. System boundaries refer to the defined limits of a system, including what is considered part of the system and what lies outside of it. This demarcation is crucial as it helps identify and assess potential security risks, vulnerabilities, and protections necessary for the information and resources within those boundaries. By clearly defining the system boundaries, an organization can prioritize its security measures, determine the scope for assessments, and manage resources effectively. Understanding where the system starts and ends allows for the implementation of appropriate security controls and policies tailored specifically to the environment in which the information systems operate. The other options are related but do not serve as the foundational means for establishing the protective scope. For instance, net-centered architecture involves how networks are structured but does not specifically define the protections for a system's data and operations. Dynamic external subsystems pertain to external components that interact with the system but don't define the scope of what needs protection. A system security plan outlines the overall strategy for protecting the system but is derived from an understanding of the system boundaries, which must be established first.

9. Which act outlines guidelines specifically for agency-wide security programs in federal agencies?

A. E-Government Act of 2002

B. Federal Information Security Management Act (FISMA)

C. Privacy Act, 1974

D. Government Information Security Reform Act (GISRA)

The Federal Information Security Management Act (FISMA) establishes a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Specifically, FISMA outlines the responsibilities of federal agencies in developing, documenting, and implementing an agency-wide information security program. This includes requirements for conducting periodic risk assessments, developing security policies and procedures, and ensuring continuous monitoring and improvement of security controls to protect federal information systems. FISMA is critical because it emphasizes the importance of an integrated security strategy, reinforcing that agency-wide security programs must adhere to specific standards and guidelines to safeguard sensitive information. This act not only mandates compliance but also requires agencies to report on the effectiveness of their security programs, thus holding agencies accountable and promoting a culture of security across the federal government. Other acts mentioned, such as the E-Government Act and the Privacy Act, focus on different areas such as improving government efficiency and protecting personal privacy, respectively. GISRA was an earlier attempt to address information security management but has been largely superseded by FISMA, which has more comprehensive guidelines. Therefore, FISMA remains the key legislation outlining guidelines for agency-wide security programs in federal agencies.

10. What form of cryptographic service is used to establish non-repudiation?

A. Symmetric Key Encryption

B. Digital Signature

C. Message Digest

D. Hashing Algorithm

Non-repudiation refers to the assurance that someone cannot deny the validity of their signature on a document or the sending of a message. Digital signatures provide this level of assurance by using asymmetric cryptography, which involves a pair of keys: a private key known only to the signer and a public key available to anyone who needs to verify the signature. When a sender wants to ensure non-repudiation, they can create a digital signature by using their private key to encrypt a hash of the message. This signature, along with the original message and the sender's public key, allows others to confirm that the message was sent by the purported sender and that it has not been altered in transit. If a dispute arises, the sender cannot deny having sent the message because only their private key could have generated that specific signature, thus establishing non-repudiation. Other forms of cryptographic services mentioned do not provide the same level of non-repudiation. Symmetric key encryption relies on a shared secret key between parties, which does not establish ownership of the message or prevent denial. Message digests and hashing algorithms are used for integrity and data verification rather than for proving origin or authenticity. They do not involve the use of keys to link a

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!