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

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. **Can the Authorizing Official delegate the decision to authorize?**

   A. True

   B. False

   C. Depends on the situation

   D. Only if there is a designated representative

2. **Which phase of the SDLC includes the implementation of security controls?**

   A. Initiation

   B. Development/Acquisition

   C. Implementation

   D. Operations/Maintenance

3. **What is the automated reporting tool that agencies must use to report data, per DHS direction?**

   A. InfoSec Reporting Tool (IRT)

   B. CyberScope

   C. Data Integrity System (DIS)

   D. Incident Reporting System (IRS)

4. **Which NIST special publication helps facilitate security control assessments in a risk management framework?**

   A. SP 800-60 Volume II

   B. SP 800-53

   C. SP 800-53a

   D. SP 800-39

5. **According to OMB M-14-04, which two individuals must sign the ATO for a new information system to operate?**

   A. CISO and CIO

   B. AO and SAOP

   C. CIO and SAOP

   D. AO and CISO

SAMPLE

6. What does the RMF Step 2 emphasize?

A. Security categorization

B. Control assessment

C. Monitoring strategy

D. Risk assessment

7. Which contingency planning variable defines the maximum time a resource can be unavailable before it impacts operations?

A. RPO

B. MTTF

C. RTO

D. RFP

8. What framework was introduced for automated assessment of security controls?

A. CyberScan

B. OCIL

C. SCAP

D. Retina

9. Which legislation requires Privacy Impact Assessments when developing new IT?

A. E-Government Act of 2002, Section 208

B. Federal Information Security Management Act (FISMA)

C. Privacy Act, 1974

D. Clinger-Cohen Act

10. What is created to correlate the information system with critical mission/business processes?

A. Risk Assessment

B. Business Impact Analysis (BIA)

C. Incident Response Plan

D. Configuration Management Plan

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Can the Authorizing Official delegate the decision to authorize?

A. True

B. False

C. Depends on the situation

D. Only if there is a designated representative

The correct answer to the question regarding whether the Authorizing Official can delegate the decision to authorize is indeed that it is false. The Authorizing Official (AO) holds a critical role in the risk management framework, responsible for making decisions about the security posture and authorization of information systems. This responsibility encompasses the decision to authorize a system for operation, which requires a comprehensive understanding of its security and risk implications. The decision to authorize is fundamentally based on the AO's judgment and accountability, representing their personal assessment of the system's security risks and compliance with security policies. Allowing delegation of this authority could undermine the integrity of the authorization process, potentially leading to misaligned risk assessments or insufficient understanding of the security implications. Therefore, while the AO can consult with other stakeholders or experts in the process of gathering relevant information to inform their decision, the final authorization must rest solely with them, ensuring accountability and security governance within the organization. This understanding emphasizes the importance of maintaining a clear chain of responsibility in federal IT security practices, highlighting why it would be inappropriate for the AO to delegate this pivotal authority.

2. Which phase of the SDLC includes the implementation of security controls?

A. Initiation

B. Development/Acquisition

C. Implementation

D. Operations/Maintenance

The correct answer focuses on the Implementation phase of the Software Development Life Cycle (SDLC), where security controls are put into place. During this phase, the actual deployment of the system occurs, and it is crucial to ensure that all security measures are applied to safeguard data and protect the system from vulnerabilities. In the Implementation phase, security controls are integrated into the system's architecture. This involves not just applying security technologies but also configuring them to ensure they operate correctly and effectively mitigate risks identified in earlier phases. Additionally, employee training and awareness programs may also be established at this point to manage human factors in security. This phase is critical because it translates theoretical security plans into practical measures. Without proper implementation of these controls at this stage, the system may be exposed to risks, which could potentially lead to data breaches and other security incidents. Other phases, such as Initiation, Development/Acquisition, and Operations/Maintenance, do involve considerations of security but do not specifically focus on the applied implementation of security controls to the same extent as the Implementation phase.

SAMPLE

3. What is the automated reporting tool that agencies must use to report data, per DHS direction?

A. InfoSec Reporting Tool (IRT)

B. CyberScope

C. Data Integrity System (DIS)

D. Incident Reporting System (IRS)

The automated reporting tool that agencies must use to report data, as directed by the Department of Homeland Security (DHS), is CyberScope. This tool is specifically designed to streamline and standardize the reporting process for cybersecurity data across federal agencies. CyberScope helps in collecting and analyzing information related to the implementation of security measures and provides insights into the cybersecurity posture of each agency. Using CyberScope ensures compliance with federal reporting requirements and enhances the ability of agencies to monitor their cybersecurity efforts systematically. It plays a crucial role in maintaining situational awareness and accountability for cybersecurity practices at the federal level. By relying on this tool, agencies can also contribute to more informed decision-making and resource allocation regarding cybersecurity initiatives. The other tools mentioned are related to different aspects of security reporting or incident management but do not serve the specific purpose of automated reporting required by DHS like CyberScope does.

4. Which NIST special publication helps facilitate security control assessments in a risk management framework?

A. SP 800-60 Volume II

B. SP 800-53

C. SP 800-53a

D. SP 800-39

The selection of SP 800-53a as the publication that facilitates security control assessments in a risk management framework is grounded in its specific purpose. NIST SP 800-53a is dedicated to providing guidelines for assessing the security controls specified in SP 800-53. It includes methodologies, assessment procedures, and templates that are important for evaluating whether the specified controls are effective in meeting security requirements. This document outlines how to conduct assessments of security controls, which is essential for ensuring that organizations effectively manage risk through their information systems. By providing detailed assessment procedures and criteria, SP 800-53a ensures that organizations can systematically evaluate the performance of their security controls, thereby supporting the overall goals of the risk management framework. In contrast, SP 800-60 Volume II focuses on categorizing information systems and mapping security controls rather than the assessment process specifically. SP 800-53 serves as the catalog of security and privacy controls but does not delve into how to assess those controls. Meanwhile, SP 800-39 provides a broader framework for managing risk within organizations but does not specifically address the operational aspects of control assessments. Therefore, the focus and purpose of SP 800-53a make it the correct choice for facilitating security control assessments within a risk

SAMPLE

5. According to OMB M-14-04, which two individuals must sign the ATO for a new information system to operate?

A. CISO and CIO

B. AO and SAOP

C. CIO and SAOP

D. AO and CISO

The correct answer is rooted in the directives outlined in OMB M-14-04, which establishes the framework for the authorization of federal information systems. The official Authorization to Operate (ATO) is a formal declaration that a system is approved to operate based on the risk assessment and security controls in place. In the context of this regulation, the individuals required to sign the ATO are the Authorizing Official (AO) and the Senior Agency Official for Privacy (SAOP). The AO is responsible for making the risk management decisions and is typically a senior official within the agency who can assume the responsibility for the security of the information system. The SAOP plays a crucial role in ensuring that the privacy of personal information is adequately protected and is integrated into the system's security assessment. Their dual sign-off on the ATO reflects the importance of both security and privacy considerations in approving the operation of information systems. This requirement underscores the necessity for cross-disciplinary engagement within federal information systems, ensuring that both security and privacy aspects are adequately addressed before a system is allowed to operate.

6. What does the RMF Step 2 emphasize?

A. Security categorization

B. Control assessment

C. Monitoring strategy

D. Risk assessment

The correct choice emphasizes that Step 2 of the Risk Management Framework (RMF) focuses on risk assessment. In this stage, organizations identify and analyze risks to their information systems. By conducting a thorough risk assessment, the organization can understand the potential impact of threats and vulnerabilities on its operations and assets. This step involves identifying security controls that can mitigate these risks and ensuring that they are effectively implemented. Step 2 is critical because it lays the foundation for the subsequent steps in the RMF process, where organizations will implement security controls based on the risks identified. Understanding the specific risks helps in prioritizing security efforts and allocating resources appropriately to protect federal information systems effectively.

SAMPLE

7. Which contingency planning variable defines the maximum time a resource can be unavailable before it impacts operations?

A. RPO

B. MTTF

C. RTO

D. RFP

The concept being addressed in this question revolves around contingency planning and the measures related to resource availability during a disruption. The correct answer relates to the Recovery Time Objective (RTO), which is a crucial metric in business continuity planning. RTO defines the maximum acceptable downtime for a resource or service before it begins to negatively affect operational capabilities. Essentially, it indicates the target time set for the recovery of IT and business activities after a disruption has occurred. Understanding the RTO helps organizations prioritize their recovery strategies and ensures that critical operations can be restored within a timeframe that minimizes adverse effects on the organization. In contrast, the other options pertain to different yet related concepts in disaster recovery and incident management. For instance, RPO, or Recovery Point Objective, deals with the maximum age of the data that can be lost in the event of a disruption, focusing specifically on data loss rather than operational downtime. MTTF, or Mean Time to Failure, refers to the average time until a system fails, and RFP is not a standard term typically used in this context. Each of these plays a role in overall recovery strategies, but only RTO specifically addresses the time limitations related to operational impact during resource unavailability.

8. What framework was introduced for automated assessment of security controls?

A. CyberScan

B. OCIL

C. SCAP

D. Retina

The correct answer is SCAP, which stands for Security Content Automation Protocol. SCAP is a suite of standards that is used for automating the assessment of security controls and is designed to facilitate the management of security-related information and to allow for automated monitoring of security configurations. SCAP combines various methods and standards such as the Common Vulnerabilities and Exposures (CVE), the Common Configuration Enumeration (CCE), and the OVAL (Open Vulnerability and Assessment Language) to establish a comprehensive framework. This framework enables organizations to automate the processes of vulnerability assessment, policy compliance, and security configuration management. By utilizing SCAP, federal agencies and other organizations can improve the efficiency of their security assessments and ensure that they adhere to regulatory requirements by automating the collection and reporting of security status information. In contrast, the other choices do not specifically represent frameworks geared toward automated assessment of security controls. CyberScan and Retina are products related to vulnerability scanning but lack the comprehensive standardization and framework that SCAP provides. OCIL (Open Checklist Interactive Language) is a language for writing checklists and can be a part of SCAP but does not encompass the entire framework for automated assessments by itself.

SAMPLE

9. Which legislation requires Privacy Impact Assessments when developing new IT?

A. E-Government Act of 2002, Section 208

B. Federal Information Security Management Act (FISMA)

C. Privacy Act, 1974

D. Clinger-Cohen Act

The E-Government Act of 2002, specifically Section 208, mandates that federal agencies conduct Privacy Impact Assessments (PIAs) when developing or procuring new information technology that collects, maintains, or disseminates personally identifiable information. This requirement emphasizes the importance of assessing privacy risks and ensuring that appropriate measures are in place to protect individuals' personal data before systems are implemented. The Act aims to enhance the management of electronic government services, ensuring transparency and accountability in how personal information is handled. By requiring PIAs, the legislation helps agencies identify potential privacy impacts from their IT projects and fosters a culture of privacy protection within the federal government. In contrast, the other options, while significant in their own right, do not specifically mandate Privacy Impact Assessments for new IT development. FISMA focuses on ensuring the security of federal information systems, the Privacy Act of 1974 provides a baseline of privacy protections for individuals, and the Clinger-Cohen Act emphasizes the need for better management and acquisition of IT resources. However, none of these explicitly require PIAs like Section 208 of the E-Government Act does.

10. What is created to correlate the information system with critical mission/business processes?

A. Risk Assessment

B. Business Impact Analysis (BIA)

C. Incident Response Plan

D. Configuration Management Plan

The Business Impact Analysis (BIA) is essential in understanding how disruptions to an information system can affect critical mission and business processes. The BIA systematically assesses the potential impacts of various disruptive events, such as natural disasters, cyber attacks, or equipment failures, on the operations of an organization. By identifying and quantifying the effects of potential interruptions, the BIA helps organizations prioritize their resources and recovery strategies. Through the BIA, organizations can determine which business processes are vital for mission success and how these processes rely on their information systems. This understanding is crucial for effective risk management and ensures that critical functions can be restored quickly after a disruption. Ultimately, the BIA contributes to developing strategies that align IT resources with business priorities, making it indispensable for integrating IT security into overall business continuity planning.

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://fitspauditor.examzify.com

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

SAMPLE