FEDERAL IT SECURITY PROFESSIONAL (FITSP) OPERATOR PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://fitspmanager.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 15

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. Which input activity involves gathering information directly from on-site stakeholders?

A. On-site interviews

B. Document reviews

C. Automated tools

D. Questionnaires and surveys

2. Which SCAP specification provides a standard naming and dictionary of system configuration issues?

A. CPE

B. CVE

C. OVAL

D. SCAP-DS

3. Which of the following is an area for adjusting system categorization?

A. Overall information system impact

B. Increasing User Population

C. Data Center Floor Space

D. Software License Count

4. What establish the scope of protection for organizational information systems?

A. System Boundaries

B. Access Control

C. Data Flow

D. Incident Response

5. RA Step 3 Task 1 focuses on communicating risk assessment results to whom?

A. Organization decision makers.

B. End users.

C. Media outlets.

D. Suppliers and contractors.

SAMPLE

6. What does DM-2 Data Retentions and Disposal support require?

A. NARA provides retention schedules that governs the disposition of federal records; program official coordinates with records officers and with NARA to identify appropriate retention periods and disposal methods

B. The organization minimizes PII collection

C. The org inventories PII

D. The org responds to privacy incidents

7. Which media sanitization step is described as the ultimate form of sanitization?

A. Disposal

B. Cleaning

C. Purging

D. Destroying

8. What is the focus of SE-1 Inventory of Personally Identifiable Information?

A. Org may extract information from PIA for information systems containing PII

B. The organization issues privacy policy updates

C. The org reports to OMB

D. The org reduces PII collection

9. Which SP 800 document focuses on the confidentiality of PII and breach response requirements?

A. Guide to Protecting the Confidentiality of PII

B. Guideline for Media Santitization

C. Information Security Handbook - A guide for managers

D. Guide to Computer Security log Management

10. What does M-03-22 Guidance for Implementing the Privacy Provisions of the E-Gov Act of 2002 cover?

A. Provides PIA guidance and requirements for all Federal agencies

B. Requires breach notification policies

C. Sets TIC standards

D. Defines encryption requirements

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which input activity involves gathering information directly from on-site stakeholders?

A. On-site interviews

B. Document reviews

C. Automated tools

D. Questionnaires and surveys

Direct, real-time input from people at the site is gathered through on-site interviews. This approach lets you talk with stakeholders who perform the work, ask follow-up questions, and observe the environment to understand workflows, controls, and concerns firsthand. It captures tacit knowledge and contextual details that documents or surveys might miss. Document reviews analyze records but don't involve stakeholders in real time; questionnaires and surveys rely on respondents who may be remote and can provide less depth; automated tools collect data without human input. Therefore, on-site interviews best meet the goal of gathering information directly from on-site stakeholders.

2. Which SCAP specification provides a standard naming and dictionary of system configuration issues?

A. CPE

B. CVE

C. OVAL

D. SCAP-DS

The main idea here is having a single, consistent way to refer to the software and hardware platforms that checks target. CPE provides exactly that: a Common Platform Enumeration, which is a formal naming scheme and a dictionary of product identifiers used across SCAP content. This standardized naming lets automated tools unambiguously reference the same platform across different datasets, catalogs, and checks, enabling reliable mapping between configurations, tests, and data. The other SCAP components serve different roles: CVE is for vulnerability identifiers, OVAL defines the language and schemas to express tests and system state, and SCAP-DS handles how data streams carry definitions and content. They don't provide the standardized product naming and dictionary that CPE offers.

3. Which of the following is an area for adjusting system categorization?

A. Overall information system impact

B. Increasing User Population

C. Data Center Floor Space

D. Software License Count

The area for adjusting system categorization is the overall information system impact. This is because security categorization uses the potential impact on operations, assets, and individuals, reflected through the combined impact across confidentiality, integrity, and availability. The overall impact level is determined by the most severe consequence in those areas, guiding how the system is categorized. Things like increasing the user population affect workload and exposure but do not by themselves change the security category. Data center floor space relates to physical housing and capacity, not security impact. Software license count pertains to procurement and capacity, not the system's security impact.

SAMPLE

4. What establish the scope of protection for organizational information systems?

A. System Boundaries

B. Access Control

C. Data Flow

D. Incident Response

System boundaries establish the scope of protection for organizational information systems. They delineate what assets, components, and data are inside the protected environment and what lies outside, guiding which security controls, policies, and monitoring apply. Once the boundary is defined, you know exactly what needs protection, what interfaces exist, and what risks to assess or mitigate. Access control, data flow, and incident response are essential security activities, but they operate within that defined boundary rather than setting the scope itself: access control enforces who can reach resources inside the boundary, data flow describes how information moves within or across boundaries, and incident response deals with events that occur within or across those boundaries. Clear boundaries help ensure consistent protection, accountability, and compliance.

5. RA Step 3 Task 1 focuses on communicating risk assessment results to whom?

A. Organization decision makers.

B. End users.

C. Media outlets.

D. Suppliers and contractors.

Communicating risk assessment results is driven by the need to equip those who govern the organization with the information they need to make decisions about risk treatment. Organization decision makers have the authority to set risk tolerance, approve mitigations, and allocate the necessary resources to address findings. When results are presented in clear, high-level terms—highlighting the current risk posture, the most significant risks, potential impact, and a prioritized set of actions—they can determine what to accept, what to mitigate, and what to accept with controls in place. End users operate within the controls and practices implemented as a result of those decisions, not the risk governance itself. External parties like media should only be involved under specific disclosure requirements, and suppliers or contractors may need some information to fulfill contracts, but they do not typically decide on risk acceptance or remediation. So the primary audience is organization decision makers who can authorize actions and resources to reduce risk.

SAMPLE

6. What does DM-2 Data Retentions and Disposal support require?

A. NARA provides retention schedules that governs the disposition of federal records; program official coordinates with records officers and with NARA to identify appropriate retention periods and disposal methods

B. The organization minimizes PII collection

C. The org inventories PII

D. The org responds to privacy incidents

DM-2 focuses on aligning data retention and disposal with federal records management requirements. NARA provides the official retention schedules that specify how long different federal records must be kept and how they should be disposed of. The program official must coordinate with records officers and with NARA to identify the appropriate retention periods for each record type and choose disposal methods that securely and properly destroy records when those periods end. This coordination ensures compliance with laws and agency policies, prevents keeping records longer than necessary, and guarantees proper disposal to protect sensitive information. While other privacy-related activities like minimizing PII collection, inventorying PII, or incident response are important, they do not address the requirement to follow retention schedules and coordinate for retention and disposal.

7. Which media sanitization step is described as the ultimate form of sanitization?

A. Disposal

B. Cleaning

C. Purging

D. Destroying

Destroying is the strongest form of sanitization because it makes the media unusable and the data unrecoverable by any practical means. After this step, there's no feasible way to read or reconstruct the information, even with advanced forensic techniques. That irreversibility is why destroying is described as the ultimate form: it goes beyond removing or overwriting data and physically renders the device incapable of being read again. Cleaning only removes dirt, and purging uses erasure methods to make recovery extremely difficult but not impossible on all media; disposing steps should follow only after proper sanitization. Destroying ensures complete, irreversible data destruction, which is essential for highly sensitive information.

8. What is the focus of SE-1 Inventory of Personally Identifiable Information?

A. Org may extract information from PIA for information systems containing PII

B. The organization issues privacy policy updates

C. The org reports to OMB

D. The org reduces PII collection

The focus is using a Privacy Impact Assessment to create and maintain an inventory of PII. A PIA describes what PII is collected, how it's used, where it's stored, and who has access for each information system. By extracting that information from PIAs, the organization can map out all PII across its information systems, detailing types of PII, where it resides, data owners, and retention. This inventory is essential for privacy risk management, accountability, and ensuring controls are in place to protect PII. Other options relate to governance or privacy goals rather than building an actual inventory. Privacy policy updates are about policy changes, not the cataloging of PII. Reporting to OMB is an oversight activity, not the inventory itself. Reducing PII collection is a privacy principle and strategy, not the act of cataloging existing PII across systems.

Sample study guide, visit https://fitspmanager.examzify.com
for the full version with hundreds of practice questions

9. Which SP 800 document focuses on the confidentiality of PII and breach response requirements?

A. Guide to Protecting the Confidentiality of PII

B. Guideline for Media Santitization

C. Information Security Handbook - A guide for managers

D. Guide to Computer Security log Management

Protecting the confidentiality of PII and handling breach response is the focus of a specific NIST SP 800 guide that targets Personally Identifiable Information. This document, commonly cited as the Guide to Protecting the Confidentiality of Personally Identifiable Information, provides a structured approach for recognizing what counts as PII, assessing the risk to its privacy, and selecting safeguards that protect its confidentiality. It covers practical controls such as data minimization, encryption, access controls, and secure handling and disposal of PII, all chosen based on the level of risk to the information. Crucially, it also addresses how to prepare for and respond to incidents involving PII, including incident detection, containment, and the steps needed to notify affected individuals or authorities as required by policy or law. The other options focus on different areas—media sanitization, broad security management guidance for managers, and log management—so they don't specifically target PII confidentiality and breach response like this guide does.

10. What does M-03-22 Guidance for Implementing the Privacy Provisions of the E-Gov Act of 2002 cover?

A. Provides PIA guidance and requirements for all Federal agencies

B. Requires breach notification policies

C. Sets TIC standards

D. Defines encryption requirements

The main idea here is that this guidance centers on privacy in federal IT by requiring careful evaluation of how personal data is collected, used, and shared. It tells agencies to perform Privacy Impact Assessments for information systems or projects that handle personal information, and to document and review privacy risks throughout the system's life cycle. It also emphasizes ensuring clear privacy notices and appropriate oversight by the CIO as part of the process. Because of this focus, the guidance is best described as providing PIA guidance and requirements for all Federal agencies. Other topics like breach notification policies, Trusted Internet Connections standards, or encryption requirements are covered by different policies and standards, not this memorandum.

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://fitspmanager.examzify.com

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

SAMPLE