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://fitspoperator.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 trio is commonly identified in continuity planning?

A. MTD, RTO, RPO

B. PKC, VPN, SSL

C. SSP, SAR, POA&M

D. Layer 3, Layer 4, Layer 7

2. The terms 'Impact and likelihood' relate to which assessment factors?

A. Risk Assessment Factors

B. SCAP Automation

C. Password Management

D. Hybrid Security Controls

3. Which resource enables automated checks against known vulnerabilities?

A. SCAP Tools

B. NVD

C. PIV

D. Authentication Header (IPSec)

4. Which SP would be the primary reference for contingency planning for federal IT systems?

A. SP 800-34

B. SP 800-63

C. SP 800-53A

D. SP 800-137

5. Which type of encryption is typically used for bulk data due to its speed?

A. Symmetric encryption

B. Asymmetric encryption

C. Hashing

D. Quantum encryption

SAMPLE

6. Which framework emphasizes policies and schedules to ensure compliance?

A. OMB IT Governance

B. FedRAMP Certification

C. FISMA Metrics

D. Disaster Recovery Steps

7. Which publication provides governance guidance for managers on information security?

A. Information Security Handbook for Managers

B. SP 800-115

C. SP 800-34

D. FIPS 198-1

8. Secure system engineering best practices are described in which publication?

A. SP 800-27 Principles

B. SP 800-53 Families

C. SP 800-34 Planning

D. NIST FIPS

9. Which term describes the minimum security requirements for federal information systems?

A. Minimum Security Baselines

B. Maximum Security Baselines

C. Security Baseline Implementation

D. Security Requirements Baseline

10. What is the Common Identification Standard for Federal Employees?

A. HSPD-12

B. FIPS 140-2

C. SCAP

D. SP 800-88

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which trio is commonly identified in continuity planning?

A. MTD, RTO, RPO

B. PKC, VPN, SSL

C. SSP, SAR, POA&M

D. Layer 3, Layer 4, Layer 7

In continuity planning, you identify time-based objectives that dictate how quickly systems must be restored and how much data you can afford to lose after a disruption. The key terms here are the maximum tolerable downtime, the recovery time objective, and the recovery point objective. The maximum tolerable downtime sets the overall limit on how long your critical functions can be unavailable before the impact becomes unacceptable. The recovery time objective translates that tolerance into a concrete target for how quickly you must bring operations back online. The recovery point objective defines how much data loss is acceptable, expressed as a time window of data that can be lost. These three together form the standard set of objectives used to shape continuity and disaster recovery strategies: you know how long you can endure downtime, you specify how fast you must recover, and you limit how much data can be lost. The other term groups are related to different domains—security documentation (system security plans, security assessment reports, plan of action and milestones) or networking layer references (OSI layers)—and they aren't the commonly identified trio used to drive continuity planning.

2. The terms 'Impact and likelihood' relate to which assessment factors?

A. Risk Assessment Factors

B. SCAP Automation

C. Password Management

D. Hybrid Security Controls

The main idea here is how risk is evaluated in security assessments. When you assess risk, you look at two key elements: the potential impact if a threat exploits a vulnerability, and the likelihood that such an event will occur. Together these determine how significant a risk is and help decide where to focus mitigations. This approach—assessing both how bad a consequence could be and how probable it is—drives prioritization of resources and controls, and is a staple in risk management frameworks like NIST RMF and ISO 31000. SCAP automation is about automated vulnerability scanning and configuration checks, not about calculating risk levels. Password management concerns how credentials are protected, not how risk is measured. Hybrid security controls describe combining different types of controls (preventive, detective, etc.), rather than the factors used to assess risk.

3. Which resource enables automated checks against known vulnerabilities?

A. SCAP Tools

B. NVD

C. PIV

D. Authentication Header (IPSec)

Automated vulnerability checks rely on a standardized framework that lets security tools run tests and compare systems to known flaws. SCAP Tools implement the Security Content Automation Protocol, bringing together data formats and exchange mechanisms used to describe vulnerabilities, configurations, and checklists. They can ingest vulnerability feeds from databases like the National Vulnerability Database and automatically verify whether assets match known issues and policy requirements. That makes SCAP Tools the best fit for automating checks against known vulnerabilities. The National Vulnerability Database provides the vulnerability data itself but does not perform automated checks. PIV is about smart card-based authentication, and an Authentication Header in IPsec is a protocol for securing traffic, not vulnerability scanning.

SAMPLE

4. Which SP would be the primary reference for contingency planning for federal IT systems?

A. SP 800-34

B. SP 800-63

C. SP 800-53A

D. SP 800-137

Contingency planning for federal IT systems is guided by NIST SP 800-34, which provides the lifecycle and actions needed to prepare for, respond to, and recover from disruptions. It lays out how to conduct a business impact analysis to determine which systems and data are essential, how to choose appropriate recovery strategies, and how to set recovery time objectives and recovery point objectives. It also covers developing and documenting contingency plans, plus testing, training, and exercises to ensure plans work when needed and remain up to date as systems change. This focus on creating, implementing, validating, and maintaining contingency capabilities is what makes SP 800-34 the go-to reference for contingency planning. The other publications address different domains: SP 800-63 focuses on digital identity and authentication, SP 800-53A covers assessment procedures for security controls, and SP 800-137 deals with information security continuous monitoring. While these are important, they do not center on the contingency planning lifecycle, making SP 800-34 the best fit for this topic.

5. Which type of encryption is typically used for bulk data due to its speed?

A. Symmetric encryption

B. Asymmetric encryption

C. Hashing

D. Quantum encryption

Symmetric encryption is used for bulk data because it is fast and efficient for large volumes. It relies on the same key to both encrypt and decrypt, which keeps the computational overhead low and allows for high-throughput processing. Algorithms like AES are specifically designed for speed and can be hardware-accelerated, making them ideal for encrypting large datasets quickly. Asymmetric encryption, while important for secure key exchange and digital signatures, is much more computationally intensive and slower, so it's not practical for encrypting large amounts of data directly. Hashing isn't encryption at all; it produces a fixed value from data to verify integrity and cannot be used to recover the original data. Quantum encryption refers to emerging techniques for securing key exchange or certain communications using quantum properties, but it's not a standard method for bulk data encryption today and also doesn't offer the same practical performance benefits for large data volumes. In practice, a common approach is to use symmetric encryption for the bulk data and asymmetric encryption to protect the symmetric key during transmission, combining speed with secure key management.

SAMPLE

6. Which framework emphasizes policies and schedules to ensure compliance?

A. OMB IT Governance

B. FedRAMP Certification

C. FISMA Metrics

D. Disaster Recovery Steps

The main idea here is governance that creates policy and sets timelines to ensure everyone follows them. OMB IT Governance focuses on establishing and enforcing IT policies across federal agencies and defining schedules for reviews, milestones, and reporting. This creates a unified policy framework and a clock for accountability, so agencies implement required controls and demonstrate compliance on a regular cadence. FedRAMP Certification is about validating cloud service providers against security baselines, which is a specific compliance activity rather than an overarching governance schedule. FISMA Metrics involve measuring and reporting how well security controls are working, not establishing the policy timing and oversight to ensure ongoing compliance. Disaster Recovery Steps cover contingency planning and getting systems back online after a disruption, not the policy governance and scheduling aspect.

7. Which publication provides governance guidance for managers on information security?

A. Information Security Handbook for Managers

B. SP 800-115

C. SP 800-34

D. FIPS 198-1

Focusing on governance and leadership for information security, this handbook is written for managers who need to shape, oversee, and sustain an information security program. It guides executives on establishing governance structures, assigning roles and responsibilities, developing policies and standards, and aligning security with business objectives. It also covers risk-based decision making, resource allocation, accountability, and continuous improvement, all from a management perspective. In contrast, the other publications are targeted at more specific areas: technical testing and assessment, contingency planning for events that disrupt operations, or cryptographic and password-related standards. None of those center on governance guidance for managers in the way this handbook does, making it the best choice for governance-focused information security guidance.

8. Secure system engineering best practices are described in which publication?

A. SP 800-27 Principles

B. SP 800-53 Families

C. SP 800-34 Planning

D. NIST FIPS

Secure system engineering is guided by engineering principles that tell you how to design and build secure IT solutions from the ground up. NIST SP 800-27 collects these IT security engineering principles and translates them into practical guidance for architecture, lifecycle practices, defense in depth, least privilege, secure defaults, and related best practices. That makes it the best reference for describing secure system engineering best practices. The other publications serve different roles: SP 800-53 provides a broad catalog of security and privacy controls to implement, SP 800-34 covers contingency planning and continuity, and FIPS publications set technical standards (like cryptographic algorithms) rather than engineering guidance.

SAMPLE

9. Which term describes the minimum security requirements for federal information systems?

A. Minimum Security Baselines

B. Maximum Security Baselines

C. Security Baseline Implementation

D. Security Requirements Baseline

The main idea here is the idea of a baseline that sets the minimum level of protection all federal information systems must meet. In federal IT security, baselines define the starting point of controls that are required to protect systems and data, ensuring a consistent, enforceable floor of security across agencies. The term "minimum" emphasizes that these are the least stringent set of requirements that must be implemented; systems can add more controls if risk dictates, but they cannot fall below this baseline. This concept is used to support compliance with FISMA and to provide a clear foundation for risk management, assessment, and authorization. That's why the term describing the minimum security requirements is the best fit. Other phrases don't capture the same standard notion: one suggests an upper limit rather than a floor, another is not the recognized label for the baseline of required protections, and the last implies a different kind of listing rather than the official starting point of controls.

10. What is the Common Identification Standard for Federal Employees?

A. HSPD-12

B. FIPS 140-2

C. SCAP

D. SP 800-88

HSPD-12 is the policy that establishes a uniform way to prove identity for federal employees and contractors, enabling secure access to facilities and information systems across all agencies. It mandates a common credential—the Personal Identity Verification card—that is used nationwide for both physical entry and logical access, with interoperable, certificate-based identity verification. The other topics focus on cryptographic modules, automated security assessment, or media sanitization, none of which define the government-wide identification standard.

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://fitspoperator.examzify.com

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

SAMPLE