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

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. **Which disaster recovery option is fully equipped and ready to take over operations quickly?**

   A. PKI Infrastructure

   B. Cold Sites

   C. Hot Sites

   D. FISMA Reporting Schedule

2. **Which standard is associated with Developing System Security Plans?**

   A. SP 800-18

   B. FIPS 181 standards

   C. FIPS 140-3

   D. PKI Components

3. **Which SP would you reference for guidance on security in public cloud environments?**

   A. SP 800-144

   B. SP 800-59

   C. SP 800-70

   D. SP 800-83

4. **Which database tracks public vulnerabilities?**

   A. NVD

   B. SCAP Tools

   C. PIV

   D. FIPS 201

5. **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

6. Self-propagating malicious code.

A. Virus

B. Worm

C. Trojan

D. Rootkit

7. Which standard defines security categorization based on impact levels for Confidentiality, Integrity, and Availability?

A. FIPS 199

B. FIPS 200

C. NIST SP 800-53

D. NIST CSF

8. What is the purpose of continuous monitoring in RMF?

A. Ongoing assessment to maintain risk posture

B. One-time security review

C. Hardware inventory only

D. Penetration testing once a year

9. Malware Prevention and Handling Guide is published as which SP?

A. SP 800-83

B. SP 800-144

C. SP 800-70

D. SP 800-59

10. SP 800-144 is associated with which concept?

A. Keyed hash for data integrity

B. Public key infrastructure

C. Cloud security guidance

D. Incident response planning

Answers

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

Explanations

1. Which disaster recovery option is fully equipped and ready to take over operations quickly?

A. PKI Infrastructure

B. Cold Sites

C. Hot Sites

D. FISMA Reporting Schedule

Disaster recovery options vary by how prepared they are to resume operations after a disruption. A hot site is a disaster recovery facility that already has the necessary infrastructure—servers, storage, networking, software, power, cooling—and often up-to-date data copies and trained staff. Because everything is in place and synchronized with the production environment, an organization can switch over with minimal downtime, meeting tight recovery objectives. This makes it the option that is fully equipped and ready to take over quickly. In contrast, a cold site provides only space and must have hardware and systems brought online, which takes more time. PKI infrastructure is about security keys and certificates, not DR readiness, and the FISMA reporting schedule concerns compliance timing, not continuity. So, the hot site best fits the requirement of being ready to take over rapidly.

2. Which standard is associated with Developing System Security Plans?

A. SP 800-18

B. FIPS 181 standards

C. FIPS 140-3

D. PKI Components

Developing a System Security Plan is guided by a standard that explicitly tells you how to document the security posture of a federal information system. The National Institute of Standards and Technology's SP 800-18, titled "Guide for Developing Security Plans for Federal Information Systems," provides the framework for building the SSP. It describes what information to capture—system boundaries, the security controls selected and implemented, responsibilities, authorization status, and how controls are assessed and monitored over time—and shows how to align the plan with the RMF process. This focus on the content and structure of the plan makes it the best fit for developing System Security Plans. The other options address different areas: FIPS 140-3 covers security requirements for cryptographic modules, FIPS 181 standards relate to PKI concepts, and PKI Components is not a formal standard for creating an SSP.

3. Which SP would you reference for guidance on security in public cloud environments?

A. SP 800-144

B. SP 800-59

C. SP 800-70

D. SP 800-83

Security guidance tailored to cloud deployments is what this item is testing. NIST SP 800-144 provides Guidelines on Security for Public Cloud Computing, offering cloud-specific considerations such as the shared responsibility model between customers and cloud service providers, data protection and encryption in the cloud, identity and access management, governance, risk management, incident response, and compliance within public cloud environments. This makes it the most appropriate reference when you need guidance that addresses the unique aspects of operating in public cloud, not just general information security controls. Other publications focus on broader federal security controls, risk categorization, or malware handling, which don't address cloud-specific security concerns in the same way.

4. Which database tracks public vulnerabilities?

A. NVD

B. SCAP Tools

C. PIV

D. FIPS 201

Public vulnerability databases collect and publish security flaws that have been disclosed so organizations can assess risk and prioritize remediation. The National Vulnerability Database is the official government repository for these disclosures. It houses CVE entries and assigns CVSS severity scores, giving a standardized way to reference and compare vulnerabilities. Maintained by NIST with feeds from MITRE, it also links to advisories and patches, and it supports automation through SCAP. That makes it the best fit for tracking publicly disclosed vulnerabilities. The other options are not databases of vulnerabilities: SCAP Tools are a set of automation tools that use vulnerability data, while PIV and FIPS 201 relate to identity verification and credentials for federal personnel, not vulnerability tracking.

5. 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.

6. Self-propagating malicious code.

A. Virus

B. Worm

C. Trojan

D. Rootkit

Self-propagating malware is designed to spread to other systems on its own, without someone needing to open a file or run a program. That behavior is the hallmark of a worm: it exploits network vulnerabilities or other propagation methods to copy itself to new machines and continue spreading autonomously. A virus, by contrast, attaches to a host file and typically requires the user to execute or activate the infected host for it to spread. A Trojan disguises itself as legitimate software to trick users into installing it, but it does not replicate by itself. A rootkit focuses on hiding its presence and maintaining privileged access, not on self-propagation.

7. Which standard defines security categorization based on impact levels for Confidentiality, Integrity, and Availability?

A. FIPS 199

B. FIPS 200

C. NIST SP 800-53

D. NIST CSF

FIPS 199 defines how information systems are categorized based on potential impact to confidentiality, integrity, and availability. It assigns impact levels—low, moderate, and high—for each CIA property and uses those to determine the system's overall security category. This categorization guides the selection of security controls, with higher impact categories requiring stronger protections. Following categorization, FIPS 200 specifies the minimum security requirements for federal information systems, aligned with the determined categories. The detailed controls are documented in NIST SP 800-53, while the NIST Cybersecurity Framework offers a voluntary, risk-based approach for managing cybersecurity that maps to outcomes but does not itself define the categorization.

8. What is the purpose of continuous monitoring in RMF?

A. Ongoing assessment to maintain risk posture

B. One-time security review

C. Hardware inventory only

D. Penetration testing once a year

Continuous monitoring is the ongoing assessment and maintenance of a system's security posture. It involves continuously collecting and analyzing security data about how controls are performing, how the environment is changing, and whether new vulnerabilities or incidents have appeared. The goal is to keep risk at an acceptable level by updating risk assessments, triggering remediation, and adjusting authorization decisions as needed. This steady, real-time view lets you detect and respond to changes—rather than waiting for a one-time audit or annual test. That's why ongoing assessment to maintain risk posture is the best description. A one-time security review doesn't capture evolving threats or changes in the system, hardware inventory alone doesn't address ongoing control effectiveness, and a penetration test conducted only once a year misses many day-to-day risks and incidents. Continuous monitoring ties everything together to sustain an approved security state.

9. Malware Prevention and Handling Guide is published as which SP?

A. SP 800-83

B. SP 800-144

C. SP 800-70

D. SP 800-59

This question asks which NIST Special Publication provides guidance on preventing malware and handling malware incidents. The publication that fits this topic is SP 800-83, which is specifically titled to address malware prevention and handling for desktops and laptops. It describes preventive controls such as anti-malware protection, timely patching, secure configurations, and user awareness, as well as the incident lifecycle—detection, containment, eradication, recovery, and lessons learned. This direct focus on preventing infections and guiding incident response makes it the best reference for malware-related practices. The other publications cover different security topics, such as wireless network security or security assessment and authorization, rather than malware prevention and incident handling.

10. SP 800-144 is associated with which concept?

A. Keyed hash for data integrity

B. Public key infrastructure

C. Cloud security guidance

D. Incident response planning

Keyed hash for data integrity is the idea here. SP 800-144 centers on using keyed-hash mechanisms, like HMAC, to ensure that data has not been altered and that the message originates from a party that knows the secret key. A keyed hash combines a cryptographic hash with a secret key so the recipient can verify both integrity and authenticity by recomputing the hash with the shared key. This approach is distinct from public key infrastructure, which relies on asymmetric cryptography and certificates; it's also different from cloud security guidance, which covers cloud-specific risk and control considerations, and from incident response planning, which focuses on detecting and responding to security incidents. So the emphasis is on protecting data integrity through keyed-hash methods.

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!