Federal IT Security Professional (FITSP) Operator Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

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. **In RA Step 2 Task 4, which elements are considered to determine likelihood?**

   A. The characteristics of the threat sources, identified vulnerabilities, and safeguards planned or implemented to impede events.

   B. Only past incident data.

   C. Budget and schedule considerations.

   D. User access controls and permissions.

2. **What does IR 7316 Assessment of Access Control System provide?**

   A. An overview and detailed information on access controls, including capabilities, limitations, and qualities of embedded access control mechanisms.

   B. A glossary of key information security terms.

   C. An overview of two novel types of smart cards that use handheld interfaces.

   D. A study on password policy and user training.

3. **Which security testing and evaluation program is used to assess security features and assurances for commercial off-the-shelf products?**

   A. Common Criteria

   B. Cryptographic Module Verification

   C. FIPS 140-2

   D. ISO 27001

4. **NIST Interagency Reports (NISTIRs) describe research of a technical nature intended for a specialized audience. True or False.**

   A. True

   B. False

   C. Not sure

   D. Both true and false

5. Which statement best describes the development life cycle relation to risk assessment?

- **A. Risk assessment is covered in all parts of the development life cycle.**
- **B. Risk assessment is performed only during deployment.**
- **C. Risk assessment is irrelevant to the development process.**
- **D. Risk assessment is done only after system retirement.**

6. What is EPHI?

- **A. Electronic Protected Health Information**
- **B. Electronic Personal Health Information**
- **C. Electronic Protected Health Insurance**
- **D. Electronic Public Health Information**

7. Following the loss of 26 million records containing PII, M-06-16 requires which of the following?

- **A. Encryption of all data on mobile devices**
- **B. Remote access only with two-factor authentication where one factor is provided by a device separate from the computer gaining access**
- **C. Use a time-out function for remote access requiring re-authentication after 30 minutes inactivity**
- **D. All of the above**

8. In what security mode are Bluetooth devices considered promiscuous?

- **A. Security Mode 1 is non-secure**
- **B. Security Mode 2 is non-secure**
- **C. Security Mode 3 is non-secure**
- **D. Security Mode 4 is non-secure**

9. Which statement best describes ISCM?

- **A. It involves defining an ISCM strategy and monitoring security controls**
- **B. It is unrelated to monitoring**
- **C. It only focuses on physical security**
- **D. It ignores training and awareness**

10. Which SP 800 document is the Technical Guide to Information Security Testing and Assessment and works with SP 800-53a for testing and assessment guidance?

A. Technical Guide to Information Security Testing and Assessment

B. Guide to Intrusion Detection and Prevention Systems (IDPS)

C. Guide for Security Focused Configuration Management of Information Systems

D. Information Security Continuous Monitoring for Federal Information System and Org

Answers

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

Explanations

1. In RA Step 2 Task 4, which elements are considered to determine likelihood?

A. The characteristics of the threat sources, identified vulnerabilities, and safeguards planned or implemented to impede events.

B. Only past incident data.

C. Budget and schedule considerations.

D. User access controls and permissions.

Likelihood is assessed by looking at three interacting factors: what threat sources are capable of and likely to do, what vulnerabilities exist that could be exploited, and what safeguards (controls) are planned or already in place to impede the event. The threat sources' characteristics tell you how plausible and damaging an attack could be; identified vulnerabilities reveal where an attacker could gain access or cause harm; safeguards show how effective defenses are at reducing or blocking that possibility. Together, these elements establish the probability that a security incident will occur. Relying only on past incident data doesn't capture the current threat landscape or the protections that may be in place now. Budget and schedule influence response and resource choices but don't directly determine how likely an event is. User access controls and permissions are important safeguards, but they're only part of the picture; you need to consider the broader mix of threats, vulnerabilities, and defenses to judge likelihood accurately.

2. What does IR 7316 Assessment of Access Control System provide?

A. An overview and detailed information on access controls, including capabilities, limitations, and qualities of embedded access control mechanisms.

B. A glossary of key information security terms.

C. An overview of two novel types of smart cards that use handheld interfaces.

D. A study on password policy and user training.

The concept being tested is how an assessment of an access control system is described and what it covers. IR 7316 focuses on evaluating access control setups by providing an overview of what access controls are and, crucially, detailed information about how embedded access control mechanisms behave. This means looking at what the system can do (its capabilities), where it might fall short or be vulnerable (its limitations), and the characteristics that make it trustworthy and effective (the qualities of the embedded controls). Understanding embedded access control mechanisms helps security teams judge how access decisions are enforced at the device level—things like hardware-anchored protections, tamper resistance, and locally enforced policy decisions—and how well these components integrate with broader security requirements. The goal is to guide a thorough assessment of whether the controls actually meet the intended security goals and where improvements might be needed. Other options describe glossary terms, new smart-card technologies, or generic policy topics, which aren't about the assessment of an access control system in the way IR 7316 covers.

3. Which security testing and evaluation program is used to assess security features and assurances for commercial off-the-shelf products?

A. Common Criteria

B. Cryptographic Module Verification

C. FIPS 140-2

D. ISO 27001

Assessing security features and assurances for commercial off-the-shelf products is done using a standardized, independent evaluation framework that defines security requirements, evaluation methods, and levels of assurance. This is provided by the Common Criteria for Information Technology Security Evaluation. It lets vendors specify what security benefits their product offers (through security targets and protection profiles) and submit to rigorous, lab-based testing and evaluation by accredited bodies to obtain a formal assurance rating (the EALs). The result is an internationally recognized certification that the product meets defined security properties. In contrast, the Cryptographic Module Verification Program focuses on validating cryptographic modules against specific cryptographic standards, such as FIPS 140-2, which is about the security of the crypto module itself rather than the broader product. ISO 27001 is about establishing and maintaining an information security management system within an organization, not evaluating a particular product's security features.

4. NIST Interagency Reports (NISTIRs) describe research of a technical nature intended for a specialized audience. True or False.

A. True

B. False

C. Not sure

D. Both true and false

NIST Interagency Reports are official publications that present technical research with detailed methods, data, and analysis for a specialized audience of researchers, engineers, and agency professionals. This focus on technical depth and targeted readership is precisely what NISTIRs are designed to convey, rather than broad-population summaries. Because of this intent and content, the statement is true. (Some NIST publications do reach broader audiences in different formats, but the defining purpose of NISTIRs is to communicate technical research to specialists.)

5. Which statement best describes the development life cycle relation to risk assessment?

A. Risk assessment is covered in all parts of the development life cycle.

B. Risk assessment is performed only during deployment.

C. Risk assessment is irrelevant to the development process.

D. Risk assessment is done only after system retirement.

Risk assessment should be integrated across the entire development life cycle, applied continuously from initial concept through design, implementation, testing, deployment, operation, maintenance, and even retirement. This ongoing approach lets you identify threats, vulnerabilities, and potential impacts early, choose appropriate controls, and adjust the risk posture as the project evolves. Relying on risk assessment only during deployment misses architectural flaws you could fix earlier, and treating risk as irrelevant or something to do after retirement would leave the system exposed and expensive to secure later. By weaving risk assessment into every phase, you create a secure by design process and maintain an up-to-date understanding of residual risk throughout the system's life.

6. What is EPHI?

A. Electronic Protected Health Information

B. Electronic Personal Health Information

C. Electronic Protected Health Insurance

D. Electronic Public Health Information

EPHI is the electronic form of protected health information. PHI covers any individually identifiable health information related to a patient's health status, treatments, or payment for care. When that information exists electronically—stored in an EHR, transmitted in email or messages, or kept in digital billing records—it becomes electronic protected health information. Because it's protected under HIPAA, EPHI requires safeguards like access controls, encryption, audit logging, and proper incident response. The other terms don't align with HIPAA terminology: using "Personal" Health Information isn't the standard label for the regulated data, "Health Insurance" shifts the focus away from the health data itself, and "Public Health Information" isn't what HIPAA protects as PHI.

7. Following the loss of 26 million records containing PII, M-06-16 requires which of the following?

A. Encryption of all data on mobile devices

B. Remote access only with two-factor authentication where one factor is provided by a device separate from the computer gaining access

C. Use a time-out function for remote access requiring re-authentication after 30 minutes inactivity

D. All of the above

Protecting PII requires layered protections that cover data at rest, data in transit, and access controls. Encrypting all data on mobile devices ensures that if a device is lost or stolen, the information it stores remains unreadable without the proper keys. Implementing remote access with two-factor authentication where one factor is provided by a device separate from the computer adds a strong barrier against credential theft, since an attacker would need both factors and cannot rely on a single stolen credential. A time-out function that requires re-authentication after 30 minutes of inactivity helps prevent someone else from taking over an unattended session. Together, these measures address multiple risk vectors and contribute to a defense-in-depth approach, making all of the above the most protective option.

8. In what security mode are Bluetooth devices considered promiscuous?

A. Security Mode 1 is non-secure

B. Security Mode 2 is non-secure

C. Security Mode 3 is non-secure

D. Security Mode 4 is non-secure

Promiscuous behavior means there's no security protection at all—the device can be discovered and connected without any authentication or encryption. In Bluetooth, that is Security Mode 1, which is non-secure. Because there's no pairing, no encryption, and no authentication, any nearby device can interact with it, making it effectively promiscuous. The other modes add layers of security (service-level or link-level) or use Secure Simple Pairing, which prevents this open, all-access behavior.

9. Which statement best describes ISCM?

A. It involves defining an ISCM strategy and monitoring security controls

B. It is unrelated to monitoring

C. It only focuses on physical security

D. It ignores training and awareness

ISCM is about establishing a plan for ongoing oversight of security controls and then continuously monitoring those controls to manage risk. It begins by defining an ISCM strategy—deciding which systems to cover, which controls to monitor, what data to collect, how often to assess, and how results will be measured and acted upon. With that plan, you implement continuous monitoring—gathering evidence from logs, scans, configurations, and test results, using dashboards and reports to spot changes, weaknesses, or new threats so you can adjust controls or authorization status as needed. That makes sense here because the essence of ISCM is the combination of a defined monitoring strategy and the ongoing assessment of security controls. It isn't about monitoring being unrelated, and it isn't limited to physical security. It also doesn't ignore training and awareness, since those elements can be part of the security controls being monitored and improved within the ISCM program.

10. Which SP 800 document is the Technical Guide to Information Security Testing and Assessment and works with SP 800-53a for testing and assessment guidance?

A. Technical Guide to Information Security Testing and Assessment

B. Guide to Intrusion Detection and Prevention Systems (IDPS)

C. Guide for Security Focused Configuration Management of Information Systems

D. Information Security Continuous Monitoring for Federal Information System and Org

The key idea is that SP 800-115 is the dedicated Technical Guide to Information Security Testing and Assessment, designed to work hand-in-hand with SP 800-53A. SP 800-115 provides the practical methods and procedures you use to plan, conduct, and analyze security testing and assessments of federal information systems. It complements SP 800-53A, which defines the assessment procedures for the security controls in SP 800-53; together, they give you the full toolkit for verifying that controls are implemented correctly and operating effectively. The other documents focus on different topics: one covers intrusions detection and prevention systems, another on secure configuration management, and another on ongoing monitoring rather than the testing and assessment process. So, the Technical Guide to Information Security Testing and Assessment is the match for testing and assessment guidance that aligns with SP 800-53A.

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!