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

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. CCE provides nomenclature and dictionary of what?

A. System security issues

B. Product names

C. Software vulnerabilities

D. Attack patterns

2. What is the primary purpose of symmetric key encryption?

A. Share a secret key, this is primarily used to achieve confidentiality

B. Public key distribution

C. Non-repudiation

D. Key escrow

3. What is the stated purpose of OMB Circular A-11?

A. Preparation, Submission and Execution of the Budget

B. Management's Responsibility for Enterprise Risk Management and Internal Control

C. Policies and Standards for executive departments and agencies to follow for financial management systems

D. Privacy Policies and Data Collection on Federal Web Sites

4. Which provision did the Computer Security Act of 1987 mandate regarding federal employees who use those systems?

A. Security awareness training

B. Mandatory encryption

C. Regular penetration testing

D. Occasional security briefings

5. What does a security assessment report provide?

A. A list of assets

B. Visibility into specific weaknesses and deficiencies in the security control that could not be resolved during development

C. A plan for new features

D. Compliance checks for external regulations

6. Which of the following is listed as a malware category?

A. Virus, Worms, Trojan Horses, Malicious Mobile Code, Tracking cookies, etc

B. Firewalls

C. Email protocols

D. Encryption standards

7. What does AR privacy control stand for?

A. Accountability, Audit, and Risk Assessment

B. Access, Review, and Retrieval

C. Audit, Risk, and Anomaly Detection

D. Accountability, Risk, and Retention

8. Which NIST IR includes the Crypto Module Validation Program and the Crypto Algorithm Validation Program?

A. IR 7536

B. IR 7358

C. IR 7816

D. IR 7581

9. In what year was the Federal Information Security Modernization Act (FISMA) enacted?

A. 1999

B. 2002

C. 2007

D. 2012

10. 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

Answers

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

Explanations

1. CCE provides nomenclature and dictionary of what?

A. System security issues

B. Product names

C. Software vulnerabilities

D. Attack patterns

CCE provides a standardized vocabulary for security configurations and misconfigurations across systems. It creates a dictionary of system security issues so that different tools and reports can reference the same issue with a common name and identifier. This consistency helps with sharing findings, mapping problems to remediation steps, and aligning with related catalogs. For example, issues like default accounts, open unnecessary ports, or insecure file permissions can be described using the same CCE identifiers across platforms and scanners. That's why the correct choice is that CCE catalogs system security issues. By comparison, product names are handled by CPE, vulnerabilities by CVE, and attack patterns by CAPEC.

2. What is the primary purpose of symmetric key encryption?

A. Share a secret key, this is primarily used to achieve confidentiality

B. Public key distribution

C. Non-repudiation

D. Key escrow

Symmetric key encryption is built around using the same secret key to both encrypt and decrypt data. The main purpose is confidentiality: as long as the key stays secret, anyone who intercepts the ciphertext cannot read the message. It's efficient for protecting large amounts of data, which is why it's widely used in secure communications. The trade-off is securely sharing the secret key between parties, which is why it's often paired with asymmetric methods for key exchange. This approach does not provide non-repudiation (that relies on digital signatures) and is not about key escrow (holding keys for later recovery).

3. What is the stated purpose of OMB Circular A-11?

A. Preparation, Submission and Execution of the Budget

B. Management's Responsibility for Enterprise Risk Management and Internal Control

C. Policies and Standards for executive departments and agencies to follow for financial management systems

D. Privacy Policies and Data Collection on Federal Web Sites

The main concept tested is what OMB Circular A-11 governs: the preparation, submission, and execution of the federal budget. A-11 provides the framework for how the government plans its budget, how agencies justify and present requests to the Office of Management and Budget, how OMB reviews and compiles those requests for submission to Congress, and how agencies implement and monitor spending once appropriations are enacted. It covers budgeting timelines, required documentation, and the controls that ensure resources are planned, justified, and tracked, linking budget decisions to program performance and accountability. Context helps: agencies must prepare budgets with clear justification and performance information, align requests with policy priorities, and manage spending within the apportionment and allotment process during execution. Other topics—such as enterprise risk management and internal controls, financial management systems standards, or privacy policies for federal websites—are addressed by different circulars and guidance (for example, internal control guidance is covered in related circulars, and financial systems or privacy policies are governed by other circulars).

4. Which provision did the Computer Security Act of 1987 mandate regarding federal employees who use those systems?

A. Security awareness training

B. Mandatory encryption

C. Regular penetration testing

D. Occasional security briefings

Security awareness training for people who use federal automated information systems is what this act established. The idea is that users are a key line of defense, so agencies must implement a security program that includes training to teach employees and contractors about their security responsibilities, appropriate use of systems, and how to recognize and respond to threats. This training helps ensure policies are followed and sensitive data is protected, addressing human factors that no technical control can fully mitigate. The other options aren't the baseline requirement the act set. It doesn't mandate encryption for all users by default, nor does it require regular penetration testing or only occasional security briefings for every user.

5. What does a security assessment report provide?

A. A list of assets

B. Visibility into specific weaknesses and deficiencies in the security control that could not be resolved during development

C. A plan for new features

D. Compliance checks for external regulations

Security assessment reports are meant to convey what weaknesses and deficiencies were found in the security controls during the evaluation and what remains unaddressed after development and testing. They lay out the specific vulnerabilities, the potential impact and likelihood, the supporting evidence, and a prioritized set of remediation steps or mitigations. The main purpose is to guide risk management decisions and drive remediation efforts, helping stakeholders understand where controls fall short and what to fix next. They aren't simply a list of assets, a plan for new features, or a broad compliance check; their value lies in providing clear visibility into security gaps and actionable directions to strengthen the controls.

6. Which of the following is listed as a malware category?

A. Virus, Worms, Trojan Horses, Malicious Mobile Code, Tracking cookies, etc

B. Firewalls

C. Email protocols

D. Encryption standards

Malware categories refer to the different types of malicious software that can harm a computer or network. The best choice lists well-known examples: viruses attach to files and spread, worms replicate themselves over networks, Trojan horses disguise themselves as legitimate software but execute harmful actions, and malicious mobile code covers harmful scripts or code that can run on devices or in web contexts. The phrase "tracking cookies" appears here as part of the broader idea of threats, but in security practice, cookies are not malware in the same sense as the other items; they're more about tracking data, while the rest are clearly malicious software. The other options describe defensive tools or standards rather than malware. Firewalls are protective barriers, not malware. Email protocols govern how messages are transmitted. Encryption standards specify how data is encoded for secrecy. So the option that lists actual malware types is the correct one.

7. What does AR privacy control stand for?

A. Accountability, Audit, and Risk Assessment

B. Access, Review, and Retrieval

C. Audit, Risk, and Anomaly Detection

D. Accountability, Risk, and Retention

AR privacy control focuses on the governance mechanisms that ensure privacy protections are actually implemented and verifiable. AR stands for Accountability, Audit, and Risk Assessment. Accountability assigns responsibility for privacy protections and outcomes. Audit provides ongoing examination and documentation to verify compliance and expose deviations. Risk Assessment identifies and evaluates privacy risks to personal data, guiding where controls are needed and what mitigations to apply. Together, these elements support transparent, traceable, and risk-based privacy management, which is why this option matches AR privacy control. The other options mix terms that aren't the standard trio: Access, Review, and Retrieval centers on data access processes; Audit, Risk, and Anomaly Detection adds Anomaly Detection, which isn't part of this AR acronym; Accountability, Risk, and Retention shifts focus to data retention rather than accountability and auditing.

8. Which NIST IR includes the Crypto Module Validation Program and the Crypto Algorithm Validation Program?

A. IR 7536

B. IR 7358

C. IR 7816

D. IR 7581

The key idea is recognizing which NIST Interagency Report actually presents both cryptographic validation programs together. The document that lays out and explains how the Crypto Algorithm Validation Program (CAVP), which tests and validates algorithm implementations, and the Crypto Module Validation Program (CMVP), which tests entire cryptographic modules against FIPS 140-2/3, are run and coordinated is the one that covers both programs in one place. It describes the scope, roles of laboratories and vendors, and the validation processes for both aspects of cryptographic assurance. That's why this IR is the best choice: it explicitly documents how these two related validation programs operate under a single umbrella. The other reports focus on different topics and do not consolidate both programs in the same way.

9. In what year was the Federal Information Security Modernization Act (FISMA) enacted?

A. 1999

B. 2002

C. 2007

D. 2012

FISMA was enacted in 2002. It was signed into law on December 17, 2002 as part of the E-Government Act, creating a standardized, risk-based information security program for federal agencies. The act established requirements for agency security planning, annual assessments, and oversight, aligning federal security practices with NIST standards. The year 2002 is the correct enactment date; the other years reflect later updates or are not the original enactment year.

10. 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.

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!