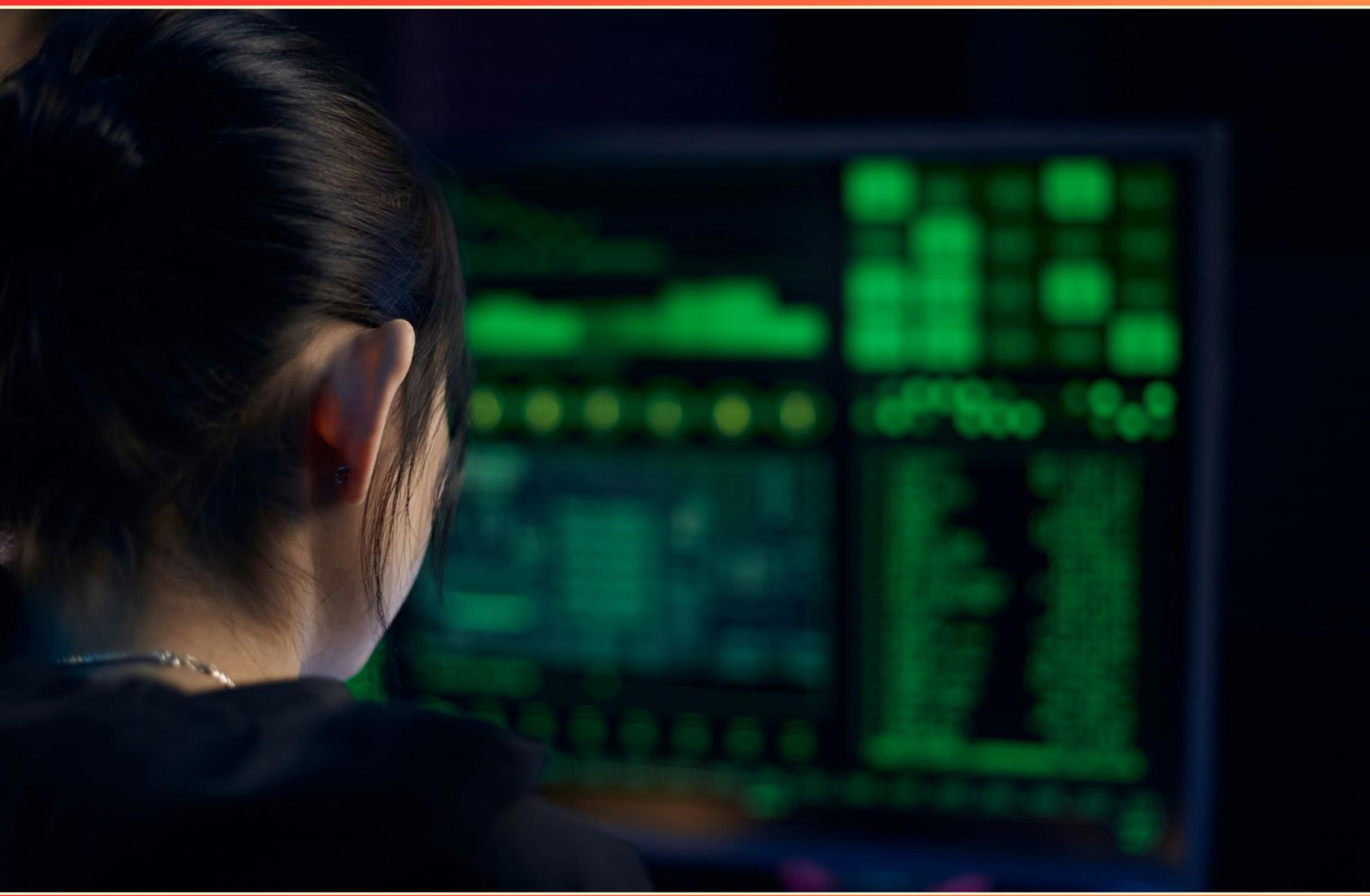
FISMA INTERVIEW PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://fismainterview.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. How many people were in your team?

A. Four

B. Six

C. Eight

D. Twelve

2. What completes the acronym C&A in the context described?

A. Certification and Accreditation

B. Compliance and Assurance

C. Cybersecurity and Access

D. Control and Authorization

3. Which of the following is the final phase in the C&A process?

A. Initiation

B. Certification

C. Accreditation

D. Monitoring

4. Which operational control is primarily about awareness and training?

A. Awareness & Training

B. Configuration Management

C. Contingency Planning

D. Incident Response

5. Accreditation boundary according to NIST SP 800-37 regroups

A. All components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected.

B. The entire organization network boundary.

C. The physical security perimeter around the data center.

D. The software component boundary within the system.

6. Which control specifically addresses interconnections between information systems?

A. CA-3 System Interconnections

B. AT-2 Security Awareness Training

C. RA-5 Vulnerability Scanning

D. FIPS 199

7. Tailoring of Security Baseline occurs when

A. When ISSO and system owner identify the Common Controls, Hybrid Controls, System Specific controls and controls not applicable; after the Draft Security Control Baseline is provided to them.

B. During system retirement.

C. After accreditation.

D. During procurement.

8. Which action is a confidentiality breach example?

A. Shoulder surfing

B. Data encryption

C. Access control

D. System patching

9. A System of Records contains information retrieved by:

A. An individual's name or other unique identifier.

B. A department code only.

C. A random access memory address.

D. A file size in bytes.

10. An interconnection security agreement (ISA) documents the technical requirements of the interconnection between what entities?

A. Between the organizations that own and operate connected IT systems

B. Between end users and IT staff

C. Between vendors and customers

D. Within a single department of an organization

Answers

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

Explanations

1. How many people were in your team?

A. Four

B. Six

C. Eight

D. Twelve

Counting the people in your team helps ensure there are enough hands to cover all necessary roles and maintain proper oversight without making coordination unwieldy. The option describing a mid-sized team is the best fit because it signals enough personnel to fill essential roles and provide backups, while still keeping communication clear and decisions timely. If the team were smaller, critical functions might lack coverage and backups; if it were larger, coordination and accountability could become more challenging. In this scenario, the described roster aligns with a mid-sized team, which is why that choice is most appropriate.

2. What completes the acronym C&A in the context described?

A. Certification and Accreditation

B. Compliance and Assurance

C. Cybersecurity and Access

D. Control and Authorization

In this context, C&A means Certification and Accreditation—the formal process used to obtain authorization to operate a system. Certification is the independent assessment that security controls are properly implemented and operating as intended. Accreditation is the formal approval by an authorizing official to operate the system, based on the certification results and the accepted level of risk. This pair is the standard terminology in federal info security (FISMA/NIST RMF) for moving a system from development to live operation: you first verify the controls (certification), then you grant official permission to operate (accreditation). The other phrases don't represent the established process used in this framework.

3. Which of the following is the final phase in the C&A process?

A. Initiation

B. Certification

C. Accreditation

D. Monitoring

Monitoring is the final phase because authorization isn't a one-time event; it relies on ongoing oversight of the system's security controls. After a system earns authorization to operate, continuous monitoring keeps track of how well those controls function, watches for new vulnerabilities, configuration changes, patch status, and incident activity, and assesses whether the risk posture remains acceptable. If changes in the system or environment raise risk or if controls weaken, the authorization decision may be revisited and reauthorization pursued. This continuous activity ensures the system stays compliant over time, making monitoring the concluding, perpetual phase in the C&A lifecycle.

4. Which operational control is primarily about awareness and training?

A. Awareness & Training

B. Configuration Management

C. Contingency Planning

D. Incident Response

The key idea here is that this control centers on people and their behavior. Awareness and training focus on ensuring everyone knows what security requires and has the skills to carry it out, from recognizing phishing attempts to following access procedures and handling data properly. This makes it the primary control for educating and preparing personnel to act securely, which is essential because human behavior is a major factor in security outcomes. In contrast, other controls deal with different aspects: configuring and maintaining system settings safely falls under configuration management, planning for emergencies and recoveries belongs to contingency planning, and having a prepared, coordinated approach to detecting and responding to incidents is the realm of incident response. Since the question emphasizes awareness and training, the control that directly addresses those needs is the Awareness & Training control.

5. Accreditation boundary according to NIST SP 800-37 regroups

A. All components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected.

B. The entire organization network boundary.

C. The physical security perimeter around the data center.

D. The software component boundary within the system.

The important idea here is what gets evaluated and approved in a security authorization. The accreditation boundary defines the scope of an information system that will be assessed and authorized by the authorizing official. It includes all components that make up the information system to be accredited, and it excludes separately accredited systems that are connected to it. This framing ensures the risk assessment and protections apply to the system as a unified package, without subsuming other systems that have their own authorizations. That's why this choice fits best: it accurately describes the boundary as the entire system to be accredited, while omitting other systems that are connected but carry their own authorization. The other options describe boundaries that are either too broad (the whole organization network), too narrow (the physical perimeter, or just the software portion), and don't reflect the formal authorization scope defined in the RMF.

6. Which control specifically addresses interconnections between information systems?

A. CA-3 System Interconnections

B. AT-2 Security Awareness Training

C. RA-5 Vulnerability Scanning

D. FIPS 199

Interconnections between information systems require a control that explicitly governs how systems connect and exchange data. The System Interconnections control is specifically designed for that purpose: it requires identifying and documenting all interconnections, obtaining proper authorization, and applying protections at the connection boundaries. It also covers interconnection security agreements and ongoing monitoring to manage risk where systems meet or share data, both internally and with external partners. This focused scope is why it best fits the question about interconnections. The other controls serve different purposes: Security Awareness Training deals with people and their behavior rather than technical links; Vulnerability Scanning targets finding weaknesses in systems; FIPS 199 provides criteria for classifying system security impact but doesn't specifically address interconnections.

7. Tailoring of Security Baseline occurs when

A. When ISSO and system owner identify the Common Controls, Hybrid Controls, System Specific controls and controls not applicable; after the Draft Security Control Baseline is provided to them.

B. During system retirement.

C. After accreditation.

D. During procurement.

Tailoring a security control baseline means adjusting the standard set of controls to fit the actual system environment and risk. This happens during the Select phase, after the Draft Security Control Baseline is provided to the ISSO and the system owner. Together they review the draft and determine which controls are common controls (inherited by the organization), which are hybrid controls, which are system-specific, and which controls are not applicable. They document the rationale and modify the baseline accordingly. This tailoring ensures the security requirements are appropriate for the system and its operations, avoiding unnecessary controls while still preserving protection. It's done before assessment and authorization, not during retirement, procurement, or after accreditation.

8. Which action is a confidentiality breach example?

A. Shoulder surfing

B. Data encryption

C. Access control

D. System patching

Confidentiality is about keeping sensitive information secret from people who shouldn't see it. Shoulder surfing—the act of someone peeking at a screen or keyboard to capture passwords, PINs, or confidential documents—directly compromises confidentiality by exposing information to an unauthorized person. The other options are protective measures: encryption makes data unreadable to unauthorized readers, strengthening confidentiality; access control limits who can access data or systems; system patching fixes security flaws to reduce exposure. In short, shoulder surfing is a breach of confidentiality because it involves unauthorized disclosure of information.

9. A System of Records contains information retrieved by:

A. An individual's name or other unique identifier.

B. A department code only.

C. A random access memory address.

D. A file size in bytes.

A System of Records is a collection of records about identifiable individuals that can be retrieved by using the person's name or another unique identifier. This means the defining feature is how you access the record—by information that uniquely points to a specific person. Among the given options, only retrieving by an individual's name or a unique identifier fits this idea, because it directly ties the data to a particular person. The other options don't fit this concept: a department code identifies an organizational unit, not a person; a random access memory address is a hardware location, not a way to locate an individual's record; and a file size is just a measurement, not an identifier used to retrieve a person's records.

10. An interconnection security agreement (ISA) documents the technical requirements of the interconnection between what entities?

A. Between the organizations that own and operate connected IT systems

B. Between end users and IT staff

C. Between vendors and customers

D. Within a single department of an organization

Interconnection security agreements focus on the security requirements for connections that cross organizational boundaries. They formalize how two or more organizations that own and operate connected IT systems will protect data as the systems interconnect, covering who is responsible for what, where the boundary lies, and which controls are required for the link. This is why describing the interconnection between the organizations that own and operate connected IT systems is the best fit. Why the other options don't fit as well: internal roles between end users and IT staff aren't about cross organizational system connections, and a vendor–customer arrangement doesn't inherently specify the technical and security requirements for interconnecting separate organizations' IT systems. Likewise, interdepartmental needs are internal to one organization and don't address inter-organizational interconnections.

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://fismainterview.examzify.com

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