FISMA Interview 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. ST&E results are described as involving which of the following actions?

A. Reporting security assessment results and issuing recommendations

B. Implementing patch management for all systems

C. Performing routine backups

D. Configuring firewall rules

2. Which publication is listed among the seven used in the past that includes SP 800-37?

A. NIST SP 800-37

B. NIST SP 800-20

C. NIST SP 800-99

D. NIST SP 800-61

3. What is an Authorization Boundary?

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

B. The boundary between internal and external networks.

C. The boundary around a data center room.

D. A boundary defined by user authentication methods.

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

A. Awareness & Training

B. Configuration Management

C. Contingency Planning

D. Incident Response

5. Who drafts the PIA according to the material?

A. The certifying agent with the ISSO

B. The System Owner

C. The CIO

D. The Security Analyst

6. Scenario: A system receives protection from controls developed by entities outside the system. This is an example of which concept?

A. Security control inheritance

B. Access control list

C. Availability

D. Integrity

7. What does a GRC tool help manage?

A. Auditing, reporting, monitoring and assessment

B. It controls payroll and HR functions.

C. Marketing campaign management.

D. Social media monitoring.

8. Which statement defines a Minor application?

A. An application, other than a major application, that requires attention to security due to the risk and magnitude of harm from loss, misuse, or unauthorized access or modification; typically included as part of a general support system.

B. A mission-critical system with strict uptime requirements.

C. A public-facing website used for marketing.

D. A personal mobile app not connected to enterprise resources.

9. What is a major application?

A. An application that requires special attention to security due to risk and magnitude of harm resulting from loss, misuse, or unauthorized access to or modification of the information in the application.

B. An application used by more than 10,000 users.

C. An application that processes only non-sensitive data.

D. An application that is open source.

10. Which grades are used on the C&A report card?

A. A for excellence and F for failure

B. B for excellence and F for failure

C. A for excellent and D for failure

D. A for achievement and F for fault

Answers

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

Explanations

1. ST&E results are described as involving which of the following actions?

A. Reporting security assessment results and issuing recommendations

B. Implementing patch management for all systems

C. Performing routine backups

D. Configuring firewall rules

ST&E results focus on the outputs produced after security testing and evaluation. They capture what was found during the assessment, assess how well security controls are working, assign risk levels, and, crucially, provide actionable guidance to mitigate weaknesses. The core purpose is to document findings and offer recommendations to management and system owners so they can decide on remediation steps and improvements. That's why reporting security assessment results and issuing recommendations is the best fit—the results themselves are the formal conclusions and guidance from the evaluation. The other actions—patch management, routine backups, and configuring firewall rules—are important security activities, but they are remediation or operational tasks that organizations implement in response to findings or as ongoing controls. They aren't the description of what ST&E results contain; the results would note whether such actions are needed and then guide what to fix, rather than being the actions themselves.

2. Which publication is listed among the seven used in the past that includes SP 800-37?

A. NIST SP 800-37

B. NIST SP 800-20

C. NIST SP 800-99

D. NIST SP 800-61

This question hinges on recognizing that there is a historical set of seven NIST SP 800-series publications that were used in the past, and SP 800-37 is part of that set. The prompt asks which publication is listed within that seven, and the publication that matches the set is SP 800-37 itself. SP 800-37 is the guide for applying the Risk Management Framework to federal information systems, which is why it appears in that foundational group. The other options refer to different NIST SP 800-series publications that cover unrelated topics and are not the publication described as being in that seven-member list.

3. What is an Authorization Boundary?

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

B. The boundary between internal and external networks.

C. The boundary around a data center room.

D. A boundary defined by user authentication methods.

An authorization boundary defines the scope of what is officially approved to operate as part of a system. It includes all components of the information system that will be authorized for operation by the authorizing official and excludes separately authorized systems to which the information system is connected. This boundary sets the exact scope for applying security controls, conducting assessments, and ongoing monitoring, ensuring the risk decisions focus on the components within the approved boundary and their interactions. Understanding this helps prevent overreach: even if the system connects to other systems, those connected systems can be kept in scope of their own authorization, while the boundary itself clearly marks what is included for this particular authorization. The other options describe different kinds of boundaries that aren't about the formal scope of an authorization—network boundaries separate internal and external networks; physical boundaries around a data center relate to facility security; and boundaries defined by authentication methods pertain to access control, not the authorized scope of operation.

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. Who drafts the PIA according to the material?

A. The certifying agent with the ISSO

B. The System Owner

C. The CIO

D. The Security Analyst

PIA stands for Privacy Impact Assessment and is part of the system authorization package. It explains how a system handles personal information and what privacy risks exist, along with the measures to mitigate them. In the certification and accreditation process, the person who leads and drafts the authorization artifacts is the certifying agent. Working with the Information System Security Officer ensures that privacy considerations are woven into the security review and that the PIA reflects both privacy and security controls. The System Owner oversees the system's operation and requirements, but the formal drafting of the PIA is carried out by the certifying agent in collaboration with the ISSO. The CIO approves the package, and the Security Analyst may contribute but does not own the drafting. So the combination of the certifying agent and the ISSO is responsible for drafting the PIA.

6. Scenario: A system receives protection from controls developed by entities outside the system. This is an example of which concept?

A. Security control inheritance

B. Access control list

C. Availability

D. Integrity

Security control inheritance occurs when protection measures for a system come from outside the system itself. Instead of implementing all controls internally, the system relies on controls provided by another organization—such as a cloud service provider, an outsourcing partner, or a third-party service. This means the system effectively inherits those external controls as part of its security posture. For example, a system hosted in a managed environment may depend on the vendor's controls for physical security, network protection, vulnerability management, and incident response. The described scenario matches this idea: protection is provided by controls developed by entities outside the system. The other terms describe different concepts. An access control list governs who can access specific resources, not where protection comes from. Availability and integrity are objectives—ensuring the system is usable when needed and that data remains accurate and trustworthy—rather than the mechanism by which protection is supplied.

7. What does a GRC tool help manage?

A. Auditing, reporting, monitoring and assessment

B. It controls payroll and HR functions.

C. Marketing campaign management.

D. Social media monitoring.

GRC tools unify governance, risk management, and compliance activities across an organization, helping teams stay aligned with policies, regulations, and business objectives. They centralize how you handle auditing, reporting, monitoring, and assessment in one place. Auditing within a GRC tool means collecting and validating evidence of control effectiveness for regulatory reviews or internal checks, making audits smoother and more consistent. Monitoring refers to continuous oversight of controls and risk indicators, so issues can be spotted and addressed early rather than after they become problems. Reporting provides dashboards and formal reports for executives, boards, and regulators, translating complex risk and compliance data into actionable insights. Assessment involves evaluating risk levels, control maturity, and policy gaps to prioritize remediation efforts and improve the overall control environment. These capabilities contrast with options focused on operational areas like payroll and HR, marketing campaign management, or social media monitoring, which are handled by specialized systems outside the governance, risk, and compliance scope.

8. Which statement defines a Minor application?

A. An application, other than a major application, that requires attention to security due to the risk and magnitude of harm from loss, misuse, or unauthorized access or modification; typically included as part of a general support system.

B. A mission-critical system with strict uptime requirements.

C. A public-facing website used for marketing.

D. A personal mobile app not connected to enterprise resources.

The idea being tested is how to classify applications by risk and importance for security in a government or agency context. A Minor application is defined as one that isn't a major system but still needs security attention because of the potential harm from loss, misuse, or unauthorized access or modification, and it's typically considered part of the general support system. This makes the statement correct because it matches both criteria: not a major, mission-critical system, yet still requiring security due to risk and being grouped under the general support framework. The other descriptions describe systems that don't fit that specific pairing: a mission-critical system would be categorized as major due to its uptime and importance; a public-facing marketing site or a personal app outside enterprise resources isn't described as part of the general support system, so they don't align with the definition of a Minor application as given.

9. What is a major application?

A. An application that requires special attention to security due to risk and magnitude of harm resulting from loss, misuse, or unauthorized access to or modification of the information in the application.

B. An application used by more than 10,000 users.

C. An application that processes only non-sensitive data.

D. An application that is open source.

A major application is one that requires heightened security because the potential harm from a breach or misuse of the information it handles is significant. This idea focuses on risk and impact: if loss, unauthorized access, or modification could cause serious damage, the application needs stronger protections and controls. The best option explicitly ties security attention to the level of risk and the possible harm to the information in the application, which is exactly what makes an application major in this sense. The other possibilities—being used by many users, processing only non-sensitive data, or being open source—do not by themselves determine that level of risk or the need for stronger security measures.

10. Which grades are used on the C&A report card?

A. A for excellence and F for failure

B. B for excellence and F for failure

C. A for excellent and D for failure

D. A for achievement and F for fault

Grading uses a simple mapping where A represents top performance and F represents failure to meet standards. On the C&A report card, the grades used are A for excellence and F for failure. This pairing reflects the standard sense of A signaling the highest quality and F signaling a fail to meet requirements. The other options mix up the meanings or use nonstandard wording (for example, using a different letter for excellence or using "fault" instead of "failure"), which is why they don't fit the established labeling.

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!