Certified Information Systems Auditor (CISA) QAE Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit:
https://cisaqae.examzify.com

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

Table of Contents

Copyright 1
Table of Contents 2
Introduction 3
How to Use This Guide 4
Questions 5
Answers 8
Explanations 10
Next Steps 16

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. **What is the purpose of integrity constraints in databases?**
   - **A. To enhance data reporting capabilities**
   - **B. To prevent entry of undefined data through validation**
   - **C. To manage user access rights**
   - **D. To improve data visualization**

2. **Utilization reports are best described as tools for:**
   - **A. Documenting hardware errors**
   - **B. Predicting resource requirements through equipment usage**
   - **C. Monitoring software performance**
   - **D. Assessing network security levels**

3. **During which SDLC phase are the business requirements of the system identified?**
   - **A. Feasibility Study**
   - **B. Requirements Definition**
   - **C. Design**
   - **D. Final Testing**

4. **What do configuration parameters allow in software?**
   - **A. They standardize software across all users.**
   - **B. They enable customization for diverse environments.**
   - **C. They restrict user access to systems.**
   - **D. They monitor system performance metrics.**

5. **Which phase focuses on verifying that project results align with original goals and deliverables?**
   - **A. Feasibility Study**
   - **B. Post-Implementation Review**
   - **C. Requirements Definition**
   - **D. Final Testing**

6. **Which type of plan is focused on recovering from IT system disruptions?**

   A. Incident Response Plan

   B. Business Continuity Plan

   C. IT Contingency Plan

   D. Digital Risk Plan

7. **Which of the following is NOT a type of biometric attack mentioned?**

   A. Replay

   B. Brute force

   C. MitM (Man-in-the-Middle)

   D. Cryptographic

8. **When should a differential backup be performed?**

   A. After a full backup has been completed

   B. Whenever data is modified significantly

   C. On a daily schedule

   D. After validating incremental backups

9. **What does the False Acceptance Rate (FAR) indicate in biometric systems?**

   A. A measure of how often valid individuals are accepted

   B. A measure of how often invalid individuals are rejected

   C. A measure of invalid individuals being accepted

   D. A measure of user satisfaction

10. **What differentiates a replay attack from a brute force attack in biometric systems?**

   A. Replay attacks use a single biometric sample.

   B. Brute force attacks re-use previous data.

   C. Replay attacks involve numerous samples at once.

   D. Brute force attacks focus on a specific strategy.

Answers

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

Explanations

1. What is the purpose of integrity constraints in databases?

A. To enhance data reporting capabilities

B. To prevent entry of undefined data through validation

C. To manage user access rights

D. To improve data visualization

Integrity constraints are rules applied to ensure the accuracy and consistency of data within a database. These constraints play a critical role in maintaining the quality of the data by preventing incorrect or undefined data entries. By implementing various types of constraints, such as primary keys, foreign keys, and unique constraints, the database enforces specific conditions that data must meet before it can be entered into the system. For instance, if a field is designated as having a unique constraint, any attempt to insert a duplicate value would be rejected, thereby ensuring that each entry remains distinct. Similarly, foreign key constraints ensure that relationships between tables are consistent, preventing orphaned records and ensuring that referenced data exists. This capability helps maintain data integrity, ensuring that the database reflects reliable and valid information. Other options, while relevant to database functionality, do not pertain directly to the role of integrity constraints. Enhancing data reporting capabilities and improving data visualization are benefits of a well-structured database but not objectives of integrity constraints. Managing user access rights relates more to security and permissions rather than the enforcement of data quality.

2. Utilization reports are best described as tools for:

A. Documenting hardware errors

B. Predicting resource requirements through equipment usage

C. Monitoring software performance

D. Assessing network security levels

Utilization reports serve as crucial instruments for analyzing equipment usage over time, allowing organizations to anticipate future resource requirements based on historical data. By examining patterns in usage, these reports help identify when equipment is heavily utilized or underutilized, facilitating more informed planning and optimization of resources. This predictive aspect is vital for ensuring that sufficient resources are available to meet anticipated demand, enabling effective management of both capacity and cost. While documenting hardware errors, monitoring software performance, and assessing network security levels are important activities in IT management, they do not align with the primary function of utilization reports. These reports specifically focus on usage trends rather than error logging, software efficiency, or security assessments. The ability to predict resource requirements is therefore the defining characteristic of utilization reports, making this the correct choice.

3. During which SDLC phase are the business requirements of the system identified?

A. Feasibility Study

B. Requirements Definition

C. Design

D. Final Testing

The phase in which the business requirements of the system are identified is the Requirements Definition phase. This phase is crucial as it serves as the foundation for the entire software development lifecycle (SDLC). During Requirements Definition, stakeholders, including business analysts, users, and project managers, collaborate to gather and document what the system must accomplish to meet business needs. In this phase, various techniques such as interviews, surveys, and workshops may be employed to extract detailed requirements. This process ensures that all stakeholder expectations are understood and articulated clearly, which helps avoid misunderstandings later in the project. The documented requirements will guide both the design and development phases that follow. By accurately capturing and defining the business requirements during this stage, organizations can achieve better alignment between the final product and the actual needs of the business, thereby reducing time and cost overruns associated with rework later in the SDLC.

4. What do configuration parameters allow in software?

A. They standardize software across all users.

B. They enable customization for diverse environments.

C. They restrict user access to systems.

D. They monitor system performance metrics.

Configuration parameters play a crucial role in software applications by enabling customization to suit various operational environments. They allow system administrators and developers to modify software behavior according to specific needs, such as adjusting settings based on a user's requirements, hardware capabilities, or organizational policies. This adaptability is essential because different users or organizations may require different configurations to optimize performance, security, or usability within their unique contexts. For example, an application used in a retail environment might need different settings compared to one used in a healthcare setting, even if they are fundamentally the same software. Utilizing configuration parameters means that clients can tailor the application to meet their specific goals, thereby enhancing functionality and ensuring that the software aligns effectively with operational demands. The other options, while containing elements related to software and its features, do not capture the primary function of configuration parameters as effectively as the ability to allow for customization in diverse environments.

5. Which phase focuses on verifying that project results align with original goals and deliverables?

A. Feasibility Study

B. Post-Implementation Review

C. Requirements Definition

D. Final Testing

The Post-Implementation Review phase is crucial because it serves as a structured approach to assess whether the outcomes of a project are in alignment with the initial goals and deliverables outlined during the project planning stages. This phase typically occurs after the project has been completed and the system or product has been deployed, allowing stakeholders to evaluate its effectiveness and efficiency in real-world usage. During the review, various criteria, including performance metrics, user satisfaction, and overall project success, are measured against the original objectives. This assessment helps organizations understand whether they met their intended goals, provides insights into what worked well, and identifies areas for improvement. By confirming that the project deliverables meet the intended requirements and objectives, organizations can enhance future project planning and implementation strategies. The other phases, such as Feasibility Study, Requirements Definition, and Final Testing, play important roles in project management but differ in focus. The Feasibility Study examines the viability of a project in terms of technical, operational, and economic aspects; the Requirements Definition phase gathers and clarifies what the project is supposed to deliver; and Final Testing ensures that the developed system or product functions as intended before it's fully deployed. These are essential processes, but they do not evaluate the alignment of the delivered outcomes with the

6. Which type of plan is focused on recovering from IT system disruptions?

A. Incident Response Plan

B. Business Continuity Plan

C. IT Contingency Plan

D. Digital Risk Plan

The correct answer is the IT Contingency Plan. This type of plan is specifically designed to address how an organization will respond to and recover from IT system disruptions. It outlines procedures and strategies to minimize the impact of unexpected events such as hardware failures, cyber-attacks, or natural disasters that could affect the availability of IT resources. An IT Contingency Plan includes detailed steps for restoring system functionality, ensuring data integrity, and maintaining business operations during and after a disruption. This focus on recovery and restoration distinguishes it from other planning documents. In contrast, an Incident Response Plan primarily focuses on managing and responding to security incidents as they occur, rather than the broader scope of recovery from disruptions. A Business Continuity Plan encompasses a wide range of activities to ensure that critical business functions can continue during a disruption, including but not limited to IT systems. The Digital Risk Plan is more focused on identifying and mitigating risks in the digital landscape rather than specifically recovering from disruptions.

7. Which of the following is NOT a type of biometric attack mentioned?

A. Replay

B. Brute force

C. MitM (Man-in-the-Middle)

D. Cryptographic

The correct answer not being a type of biometric attack is indeed associated with the concept of a Man-in-the-Middle (MitM) attack. Biometric attacks are typically those that directly target biometric systems or the data associated with them. A replay attack involves capturing and reusing valid biometric data to gain unauthorized access, directly challenging the integrity of biometric authentication systems. A brute force attack, on the other hand, could be relevant in the context of trying various biometric samples (for example, copies of fingerprints) until a match is found, aiming to bypass biometric security. Cryptographic attacks are more about exploiting weaknesses in encryption algorithms or protocols rather than directly attacking the biometric characteristics themselves. While they can be related due to the use of biometrics within cryptographic systems, they do not describe the act of manipulating biometric data specifically. In contrast, a MitM attack focuses on intercepting and potentially altering communications between two parties without their knowledge, which does not specifically target the biometric elements involved in authentication processes. Thus, it does not classify as a biometric attack.

8. When should a differential backup be performed?

A. After a full backup has been completed

B. Whenever data is modified significantly

C. On a daily schedule

D. After validating incremental backups

A differential backup is designed to capture all the changes made to the data since the last full backup. Therefore, it should be performed after a full backup has been completed. This practice ensures that the differential backup contains all the modifications that have occurred since the last full backup, making it easier to restore the data to the most recent state. To clarify further, while performing differential backups on a daily schedule might seem practical, it's not a necessity as they only need to occur after a full backup. Similarly, performing them whenever data is modified significantly is not an effective strategy as it could lead to data consistency issues, particularly if multiple differential backups crowd together in close timeframes. Lastly, validating incremental backups is essential for ensuring data integrity, but it doesn’t directly influence the timing of when to perform a differential backup, which is specifically tied to the completion of the last full backup. Thus, the most accurate guideline for scheduling a differential backup is indeed the completion of a full backup.

9. What does the False Acceptance Rate (FAR) indicate in biometric systems?

A. A measure of how often valid individuals are accepted

B. A measure of how often invalid individuals are rejected

C. A measure of invalid individuals being accepted

D. A measure of user satisfaction

The False Acceptance Rate (FAR) is a crucial metric in biometric systems that quantifies how often the system mistakenly grants access to an unauthorized user. It specifically measures the scenario where an invalid individual is incorrectly accepted as a valid one, which can lead to security breaches. A higher FAR indicates a greater likelihood of a security risk, meaning that the system is less reliable in distinguishing between legitimate users and impostors. In the context of biometric systems, understanding the FAR helps organizations assess the effectiveness and reliability of their authentication measures. It allows them to balance security with usability, ensuring that while valid users are granted access, the risk of intruders being falsely granted access is minimized. FAR is distinctly different from measures like the False Rejection Rate (FRR), which assesses how often valid individuals are denied access. Thus, the correct answer emphasizes the significant security implications associated with the FAR in biometric authentication processes.

10. What differentiates a replay attack from a brute force attack in biometric systems?

A. Replay attacks use a single biometric sample.

B. Brute force attacks re-use previous data.

C. Replay attacks involve numerous samples at once.

D. Brute force attacks focus on a specific strategy.

A replay attack is characterized by its use of a single biometric sample that has been captured and re-used to gain unauthorized access. In this attack, an attacker captures a legitimate user's biometric data, such as a fingerprint or facial recognition data, and then attempts to use that same data to impersonate the user. The essence of a replay attack lies in the act of collecting and reusing a valid authentication data point, which is typically done without requiring any alteration or generation of new data. This contrasts with brute force attacks, which systematically attempt all possible credentials or combinations. In the context of biometric systems, a brute force attack would involve testing various biometric samples or characteristics continuously until the correct one is found, rather than relying on a previously captured sample. The clarification of the differences is critical, as it aids in understanding the defenses necessary for biometric systems. Replay attacks can be mitigated by using techniques like nonces or timestamps, while brute force attacks require more robust mechanisms, such as limiting the number of attempts or introducing additional forms of authentication. Thus, identifying the distinctions between the two types of attacks helps in implementing suitable security measures.

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://cisaqae.examzify.com

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