CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA) QAE PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cisaqae.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

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

SAMPLE

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

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. What does compliance testing aim to achieve?

A. To evaluate user satisfaction

B. To gather evidence of regulatory compliance

C. To enhance software performance

D. To improve system architecture

2. Which of the following accurately describes the False Rejection Rate (FRR) in biometrics?

A. A measure of valid individuals being accepted

B. A measure of invalid individuals being rejected

C. A measure of how often valid individuals are rejected

D. A measure of overall biometric accuracy

3. What is the primary objective of the feasibility study in the SDLC?

A. To identify the technical requirements of the system

B. To determine the strategic benefits and organizational impact of the project

C. To outline the project management practices

D. To assess the training needs for the project team

4. What is a significant benefit of limit checks in data entry?

A. They enhance data processing speed

B. They prevent the entry of invalid data

C. They allow for easy data retrieval

D. They minimize user training needs

5. In a biometric security context, which focus is critical for preventing replay attacks?

A. Currently used algorithms

B. Live data processing

C. Environmental controls

D. User access management

SAMPLE

6. What does normalization in database management primarily aim to remove?

A. Duplicated data elements

B. All transactional data

C. Unsecured data points

D. User access logs

7. What is one of the weaknesses that a replay attack exploits?

A. Weak encryption

B. Stored biometric characteristics

C. Live biometric capture

D. Detection of spoofing

8. What is considered the greatest risk associated with USB drives?

A. Data corruption

B. Malware infections

C. Theft of the devices

D. Firmware bugs

9. Which SDLC phase is primarily concerned with design for systems developed internally?

A. Phase 3A

B. Phase 3B

C. Phase 5

D. Phase 6

10. What role does an organization's CSIRT play in cybersecurity?

A. Performing system backups

B. Disseminating security updates and guidelines

C. Conducting penetration testing

D. Creating firewall policies

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does compliance testing aim to achieve?

A. To evaluate user satisfaction

B. To gather evidence of regulatory compliance

C. To enhance software performance

D. To improve system architecture

Compliance testing primarily aims to gather evidence of regulatory compliance. This type of testing is fundamentally about ensuring that an organization's processes, systems, and controls adhere to the specific laws, regulations, standards, and internal policies that apply to its operations. By conducting compliance testing, organizations can identify whether they meet the necessary legal and regulatory requirements, which is critical for avoiding penalties, maintaining operational integrity, and delivering transparent reporting to stakeholders. Compliance testing involves validating that controls are in place and functioning as intended to meet these obligations. The information obtained from this testing can help management understand the risk of non-compliance and take proactive measures to address any gaps or deficiencies that may exist. This forms a crucial part of an organization's governance, risk management, and compliance (GRC) framework. In contrast, the other options focus on areas not directly related to assessing adherence to standards or regulations. User satisfaction pertains to user feedback and experiences with the system, performance enhancement is about optimizing systems for better efficiency or speed, and improving system architecture involves redesigning or restructuring system components for better integration and function, none of which directly evaluate compliance to regulations.

2. Which of the following accurately describes the False Rejection Rate (FRR) in biometrics?

A. A measure of valid individuals being accepted

B. A measure of invalid individuals being rejected

C. A measure of how often valid individuals are rejected

D. A measure of overall biometric accuracy

The False Rejection Rate (FRR) is an important concept in biometric systems, defined as the measure of how often valid individuals are incorrectly rejected by the system. This metric is crucial for understanding the system's performance, particularly in terms of user convenience and satisfaction; a high FRR can lead to frustration for legitimate users who are repeatedly denied access. FRR is typically calculated by taking the number of false rejections (instances when a legitimate user is denied access) and dividing it by the total number of times legitimate users attempt to gain access. This provides an understanding of the likelihood that a valid user will face erroneous denial, impacting user experience significantly. Understanding FRR helps organizations assess the balance between security and accessibility in their biometric systems, ensuring that while security measures are robust, they do not interfere unduly with authorized users' ability to access the system.

SAMPLE

3. What is the primary objective of the feasibility study in the SDLC?

A. To identify the technical requirements of the system

B. To determine the strategic benefits and organizational impact of the project

C. To outline the project management practices

D. To assess the training needs for the project team

The primary objective of the feasibility study in the System Development Life Cycle (SDLC) is to determine the strategic benefits and organizational impact of the project. This phase is crucial as it analyzes not just whether the project is technically possible, but also whether it aligns with the organization's goals and strategic plan. A feasibility study examines various aspects including economic viability, technical feasibility, legal considerations, and operational impacts. By focusing on the strategic benefits, the feasibility study ensures that the project's outcomes will support the broader objectives of the organization, making it a vital step in decision-making before investing significant resources and moving forward with development efforts. This assessment helps stakeholders understand how the project may contribute to the organization's success, including potential return on investment, alignment with business goals, and overall impact on operations. The other options, while relevant to project planning and execution, do not capture the overarching goals of the feasibility study as comprehensively as the determination of strategic benefits and organizational impact. Identifying technical requirements is certainly part of project development but plays a smaller role in justifying the project's direction at the feasibility stage. Outlining project management practices and assessing training needs are also important but are typically addressed in later stages of the project once feasibility has been established.

4. What is a significant benefit of limit checks in data entry?

A. They enhance data processing speed

B. They prevent the entry of invalid data

C. They allow for easy data retrieval

D. They minimize user training needs

Limit checks in data entry serve a critical role by ensuring that only valid data falls within predetermined thresholds or ranges. This means that if a user tries to input a value that exceeds the established limits—be it a numeric entry that is too high or a date that is out of a specified range—the system will flag this entry as invalid, prompting the user to correct it. By doing so, limit checks significantly enhance data quality and integrity, preventing errors that may occur from improper data entry. This feature is vital for maintaining accurate databases and for ensuring that subsequent processes that rely on this data—such as reporting and decision-making—are based on correct and reliable information. While other options may offer benefits in different contexts, the primary function of limit checks is centered around validating the input data, thereby reinforcing the necessity of option B as the correct answer.

SAMPLE

5. In a biometric security context, which focus is critical for preventing replay attacks?

A. Currently used algorithms

B. Live data processing

C. Environmental controls

D. User access management

In a biometric security context, focusing on live data processing is critical for preventing replay attacks. Replay attacks occur when an attacker captures and reuses biometric data, such as fingerprints or facial recognition data, to gain unauthorized access. By employing live data processing, biometric systems can verify that the biometric input is being generated from a live user at the time of authentication rather than from a recorded sample or a spoofed source. This is typically achieved through techniques such as liveness detection, which can assess physiological indicators that confirm the presence of a real person, such as heart rate, temperature changes, or movements that are difficult to replicate with static images or recordings. This additional layer helps in ensuring that the biometric system is responding to a genuine biometric input, thus effectively thwarting attempts to use previously captured data for unauthorized access. While currently used algorithms are important for the overall effectiveness and accuracy of biometric systems, they do not inherently address the specific risk of replay attacks. Environmental controls and user access management also play roles in security but are not as directly related to the prevention of replay attacks as live data processing is. Therefore, the emphasis on live data processing is fundamental in enhancing the security provided by biometric systems against such vulnerabilities.

6. What does normalization in database management primarily aim to remove?

A. Duplicated data elements

B. All transactional data

C. Unsecured data points

D. User access logs

Normalization in database management primarily aims to remove duplicated data elements. The process of normalization involves organizing the database structure to reduce redundancy and improve data integrity. By ensuring that each piece of data is stored in only one location, normalization minimizes the chances of inconsistencies and anomalies that can arise when the same piece of information is stored in multiple places. Through various normal forms—such as first normal form (1NF), second normal form (2NF), and third normal form (3NF)—the technique establishes rules for how data should be structured to eliminate duplicate data across tables, ensuring that each table focuses on a single subject or entity. This not only optimizes storage but also enhances the efficiency of database operations, such as querying and updating data. The other options presented do not align with the primary goal of normalization. Transactional data is essential for operations and is not something normalization seeks to remove. Unsecured data points pertain to security concerns, which is not an aspect of the normalization process. Similarly, user access logs are important for security auditing and management, and are not addressed through normalization.

SAMPLE

7. What is one of the weaknesses that a replay attack exploits?

A. Weak encryption

B. Stored biometric characteristics

C. Live biometric capture

D. Detection of spoofing

A replay attack is a type of network security attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. One of the key weaknesses that a replay attack exploits is the use of stored biometric characteristics. In the case of biometric authentication systems, if an attacker is able to capture the data transmission that includes a user's biometric information (such as fingerprint or facial recognition data), they could later replay that data to gain unauthorized access. The security of such systems heavily relies on the uniqueness and timely capture of biometric data, as well as the system's ability to differentiate between live biometric input and stored data. Stored biometric characteristics can be vulnerable because they do not inherently change and can be intercepted. In contrast, systems that require live biometric capture are better equipped against replay attacks, as they analyze the data in real-time and can look for signs of liveness, thus reducing the risk associated with repeated or delayed transmissions of previously captured data. Understanding this dynamic highlights the importance of implementing security mechanisms that protect against replay attacks, particularly in systems relying on biometrics for authentication.

8. What is considered the greatest risk associated with USB drives?

A. Data corruption

B. Malware infections

C. Theft of the devices

D. Firmware bugs

The greatest risk associated with USB drives is the theft of the devices. USB drives are small and easily portable, making them susceptible to being lost or stolen. When a USB drive is taken, it can lead to unauthorized access to sensitive information stored on it, which can result in data breaches. This risk is particularly significant in environments where employees may handle sensitive data, as lost or stolen drives can expose organizations to legal, financial, and reputational damage. While data corruption, malware infections, and firmware bugs are valid concerns, they tend to be specific to the condition and use of the device rather than representing the overarching risk posed by the physical nature of USB drives. The potential for theft highlights the importance of implementing robust data protection measures, such as encryption and access controls, to safeguard information stored on removable media.

SAMPLE

9. Which SDLC phase is primarily concerned with design for systems developed internally?

A. Phase 3A

B. Phase 3B

C. Phase 5

D. Phase 6

The correct choice focuses on Phase 3B of the Software Development Life Cycle (SDLC), which is specifically directed towards the detailed design of systems that are developed internally. This phase involves taking the conceptual framework established in earlier phases and creating detailed specifications that include systems architecture, data structures, interfaces, and other component designs necessary for development. During Phase 3B, the designers work closely with stakeholders to ensure that all functional requirements are effectively transformed into detailed design documents. This meticulous design phase ensures that the system will meet end-user needs and fit appropriately into the overall system architecture. It also helps in identifying potential risks and any organizational constraints that may affect the development process. This is the stage where clarity on how the system will be built takes precedence, paving the way for the subsequent phase of implementation. Therefore, understanding this distinction is crucial for grasping how the SDLC guides the progress from initial requirements to actual system design, focusing on internal development.

10. What role does an organization's CSIRT play in cybersecurity?

A. Performing system backups

B. Disseminating security updates and guidelines

C. Conducting penetration testing

D. Creating firewall policies

The primary role of an organization's Computer Security Incident Response Team (CSIRT) is to respond to security incidents effectively. This includes disseminating security updates and guidelines, which is essential for maintaining a robust cybersecurity posture. The CSIRT acts as a central point of coordination for incident response activities, ensuring that the latest information about vulnerabilities, patches, and security best practices is communicated to all relevant stakeholders within the organization. By providing timely updates and guidelines, the CSIRT helps to mitigate risks associated with known vulnerabilities, ensuring that employees and systems are informed and adequately prepared to defend against potential threats. This proactive communication is vital for enhancing the overall security awareness throughout the organization and fostering a culture of vigilance against cyber threats. While other options like performing system backups, conducting penetration testing, and creating firewall policies are important components of cybersecurity practices, they fall outside the primary responsibilities of a CSIRT. Instead, these tasks are typically handled by other specialized teams or departments within the organization. The focus of the CSIRT specifically on incident response and communication around security guidelines distinguishes its role in the cybersecurity framework.

SAMPLE

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!

SAMPLE