CISA Domain 4 Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

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

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. **In a relational database with referential integrity, which key prevents the deletion of a row from a customer table while referencing it in orders?**

   A. Foreign key

   B. Primary key

   C. Secondary key

   D. Public key

2. **What control should an IS auditor recommend to avoid out-of-range data in a database?**

   A. Log all table update transactions

   B. Implement integrity constraints in the database

   C. Implement before and after image reporting

   D. Use tracing and tagging

3. **Which process is most effective in reducing the risk of unauthorized software being distributed to a production server?**

   A. Manually copy files to accomplish replication.

   B. Review changes in the software version control system.

   C. Ensure that developers do not have access to the backup server.

   D. Review the access control log of the backup server.

4. **The activation of a business continuity plan should be based on which of the following?**

   A. Duration of the outage

   B. Type of outage

   C. Probability of the outage

   D. Cause of the outage

5. **What must be established for an organization's disaster recovery plan to effectively address system prioritization following a disaster?**

   A. All information systems need to be prioritized

   B. General user management must determine system priority

   C. The IS manager should designate recovery priorities

   D. Only critical financial systems should be prioritized

6. When analyzing database transaction logs, which outcome indicates a violation of atomicity?

- **A. All transactions executed solely through external interfaces.**
- **B. Some transactions remain partially executed without rollback.**
- **C. Transactions are executed concurrently leading to data inconsistencies.**
- **D. Database states reflect a correct transition after processing.**

7. During the reconciliation of separate business continuity plans for different departments, what should be addressed first?

- **A. Evacuation plan**
- **B. Recovery priorities**
- **C. Backup storages**
- **D. Call tree**

8. What should an IS auditor evaluate to ensure personnel are aware of their emergency roles?

- **A. Current business policies**
- **B. Results from continuity tests**
- **C. Training documentation**
- **D. Emergency contact lists**

9. In an IT disaster recovery plan, what should the IS auditor primarily ensure is covered?

- **A. A resilient IT infrastructure.**
- **B. Information on alternate sites.**
- **C. Documented disaster recovery test results.**
- **D. Analysis and prioritization of business functions.**

10. What should an IS auditor do when they notice continuous addition of storage resources in IT infrastructure?

- **A. Recommend the use of disk mirroring.**
- **B. Review the adequacy of offsite storage.**
- **C. Review the capacity management process.**
- **D. Recommend the use of a compression algorithm.**

Answers

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

Explanations

1. **In a relational database with referential integrity, which key prevents the deletion of a row from a customer table while referencing it in orders?**

   A. Foreign key

   B. Primary key

   C. Secondary key

   D. Public key

In a relational database, referential integrity ensures that relationships between tables remain consistent. When a record in one table references a record in another table, any operation—such as deletion—on the referenced table must maintain this integrity. In the scenario described, the customer table and orders table are related. The foreign key in the orders table corresponds to the primary key in the customer table, establishing a link between the two. This foreign key constraint prevents the deletion of a row from the customer table if there are still orders linked to that customer. If an attempt to delete a customer is made while there are existing related orders, the database will reject the deletion to maintain referential integrity. The primary key uniquely identifies each record in a table but does not enforce any constraints regarding other tables' dependencies. The secondary key serves the purpose of facilitating data retrieval based on non-primary key columns but also does not enforce referential integrity. Lastly, a public key is unrelated to the concepts of database keys; it is typically associated with encryption and data security. Thus, the foreign key serves the critical function of preserving referential integrity between the customer and orders tables by preventing the deletion of a customer record that is still referenced, making it the appropriate choice.

2. **What control should an IS auditor recommend to avoid out-of-range data in a database?**

   A. Log all table update transactions

   B. Implement integrity constraints in the database

   C. Implement before and after image reporting

   D. Use tracing and tagging

Implementing integrity constraints in the database is the most effective control to avoid out-of-range data. Integrity constraints are rules established within a database to ensure the accuracy and consistency of the stored data. These constraints can specify acceptable values for a field, such as defining a range for numerical data or requiring that certain fields must be present (not null). By setting these parameters, the database will automatically reject any data entries that do not conform to the specified rules, thus preventing out-of-range values from being accepted in the first place. Logging all table update transactions, while useful for auditing and tracking changes, does not prevent out-of-range data from being entered initially. Instead, it serves as a post-facto measure to identify issues after they have occurred. Implementing before and after image reporting allows an auditor to see how data has changed over time, which can be helpful for tracking alterations, but it does not prevent incorrect data from being entered in a database in the first place. Using tracing and tagging can aid in monitoring and resource management but does not address the fundamental issue of data integrity within the database itself. Thus, integrity constraints are crucial for ensuring that all data adheres to the defined criteria, safeguarding the quality and reliability of the data held within the database.

3. Which process is most effective in reducing the risk of unauthorized software being distributed to a production server?

A. Manually copy files to accomplish replication.

B. Review changes in the software version control system.

C. Ensure that developers do not have access to the backup server.

D. Review the access control log of the backup server.

The most effective process for reducing the risk of unauthorized software being distributed to a production server is to review changes in the software version control system. This method provides a structured and systematic approach to software development and deployment by tracking all changes made to the codebase. The version control system records every modification, including who made the changes, what was altered, and when the changes took place. This transparency significantly mitigates risks, as it allows for thorough auditing and accountability. By leveraging this process, organizations can ensure that only approved and thoroughly reviewed code is deployed to production servers. Any unauthorized or malicious changes can be detected and addressed before deployment, thereby enhancing the security of the software supply chain. Additionally, version control systems often include approval mechanisms, which can further reinforce the security measures in place. In contrast, manually copying files lacks oversight and logging, making it difficult to track unauthorized changes. Ensuring that developers do not have access to the backup server may not effectively address the problem of unauthorized software distribution, as it does not control how software is developed or deployed. Reviewing access control logs is useful for monitoring actions taken on a system, but it does not proactively prevent unauthorized software from being introduced into the production environment. Therefore, relying on version control is the most comprehensive

4. The activation of a business continuity plan should be based on which of the following?

A. Duration of the outage

B. Type of outage

C. Probability of the outage

D. Cause of the outage

The activation of a business continuity plan should be based on the duration of the outage because it directly impacts the organization's ability to continue its critical operations. When assessing whether to activate a business continuity plan, understanding how long a system or service will be unavailable is essential. A short outage may not necessitate a full activation of the continuity plan, whereas a prolonged outage could severely affect operations, customer satisfaction, and revenue generation, thus requiring a comprehensive response. Choosing to activate based on the duration allows organizations to prioritize their resources and actions effectively. It helps in determining the level of response needed — for instance, whether to switch to a recovery site, implement remote work solutions, or engage alternate suppliers. This consideration ensures that the organization can manage the situation appropriately while minimizing risks and impacts.

5. **What must be established for an organization's disaster recovery plan to effectively address system prioritization following a disaster?**

   A. All information systems need to be prioritized

   B. General user management must determine system priority

   C. The IS manager should designate recovery priorities

   D. Only critical financial systems should be prioritized

To effectively address system prioritization following a disaster, it is essential that clear guidelines and decision-making processes are established. In this context, having general user management take the lead in determining system priorities is crucial because they possess insights into the operational needs and dependencies across various functions of the organization. This collaborative approach ensures that the disaster recovery plan aligns with the organization's overall business objectives and operational criticality. User management is typically aware of which systems are essential for business continuity and can prioritize them according to their impact on daily operations. This collective input can help avoid potential biases that might arise if only one group's perspective is considered. By involving user management, the disaster recovery plan can more accurately reflect the needs of the entire organization, allowing for a more effective and efficient recovery process. Establishing prioritization based solely on the views of a single individual, such as the IS manager, or focusing only on critical financial systems could overlook vital operational areas and lead to improper recovery strategies. Thus, engaging broader user management creates a holistic understanding of system dependencies, ensuring that the recovery plan is robust and comprehensive.

6. **When analyzing database transaction logs, which outcome indicates a violation of atomicity?**

   A. All transactions executed solely through external interfaces.

   B. Some transactions remain partially executed without rollback.

   C. Transactions are executed concurrently leading to data inconsistencies.

   D. Database states reflect a correct transition after processing.

The choice indicating a violation of atomicity is indeed the scenario where some transactions remain partially executed without rollback. Atomicity is one of the key properties of database transactions, often described by the acronym ACID (Atomicity, Consistency, Isolation, Durability). In the context of atomicity, a transaction must be completely executed or not executed at all; it cannot be left in an incomplete state. When transactions are partially executed, it means that they have not fully completed or failed, and this state can lead to data inconsistencies, corrupt states, and uncommitted changes within the database. A situation where some transactions are only partially completed without rollback clearly violates atomicity. It shows that not all parts of a transaction were successfully completed, contradicting the very essence of what atomic transactions are designed to achieve. In a properly functioning database adhering to atomicity principles, if a transaction fails at any stage, any of the changes it made must be reverted, ensuring that all operations succeed or none at all. The other options don't reflect violations of atomicity. Transactions executed solely through external interfaces can still maintain atomicity as long as they are managed properly. Concurrent transactions can occur without violating atomicity, provided that isolation mechanisms are effectively employed to maintain data

7. During the reconciliation of separate business continuity plans for different departments, what should be addressed first?

A. Evacuation plan

B. Recovery priorities

C. Backup storages

D. Call tree

In reconciling separate business continuity plans, addressing the evacuation plan first is crucial because it sets the foundation for ensuring the safety of personnel during a crisis. The evacuation plan outlines the procedures for safely exiting the building or area in the event of an emergency, prioritizing human life above all else. This step is vital for minimizing risk and ensuring that all employees understand how to respond in emergencies, creating a safer environment for subsequent recovery activities. Understanding evacuation processes helps ensure that all departments align their plans with a shared safety protocol, which is essential for effective communication and coordination during an emergency. Once the evacuation procedures are established, the organization can then address more detailed aspects like recovery priorities, backup storage, and communication methods such as call trees. Each of these components is important, but initiating the discussion with evacuation ensures that the well-being of all individuals is the primary focus at the onset of the business continuity planning process.

8. What should an IS auditor evaluate to ensure personnel are aware of their emergency roles?

A. Current business policies

B. Results from continuity tests

C. Training documentation

D. Emergency contact lists

To ensure that personnel are aware of their emergency roles, evaluating training documentation is crucial. This documentation captures all the information and guidance provided to employees regarding their responsibilities during emergencies. It typically includes training records, materials used in training sessions, and schedules of trainings conducted, detailing what was covered and when. By reviewing this documentation, an IS auditor can verify whether employees have received adequate training on their specific roles in an emergency, ensuring they understand the actions required of them and the protocols to follow. Effective training documentation not only outlines these roles but also signifies that the organization is committed to preparing its personnel for emergencies. This preparation is vital for effective incident response and continuity of operations. Evaluating current business policies, results from continuity tests, or emergency contact lists, while important in their respective contexts, do not directly assess whether staff are aware of their specific roles during emergencies. Business policies might provide a framework, continuity tests indicate the effectiveness of plans, and contact lists support communication; however, they do not confirm the level of understanding employees have of their assigned emergency responsibilities.

9. In an IT disaster recovery plan, what should the IS auditor primarily ensure is covered?

A. A resilient IT infrastructure.

B. Information on alternate sites.

C. Documented disaster recovery test results.

D. Analysis and prioritization of business functions.

In an IT disaster recovery plan, the focus should be on the analysis and prioritization of business functions because this step is critical for ensuring that resources are allocated effectively when a disaster occurs. An IS auditor must verify that the organization understands which business functions are essential for operations, which can be restored quickly, and which can afford to have a longer recovery time. This prioritization helps in making informed decisions about where to invest in recovery resources and reduces downtime, ultimately ensuring business continuity. Understanding the importance of business functions allows organizations to tailor their disaster recovery strategies to meet the unique needs of their operations, aligning recovery efforts with the overall business objectives. This leads to more efficient recovery processes, minimizing impacts on critical services and systems. While elements like a resilient IT infrastructure, information on alternate sites, and documented test results are important, they serve to support the primary goal of maintaining essential business functions, making them secondary to the need for thorough analysis and prioritization.

10. What should an IS auditor do when they notice continuous addition of storage resources in IT infrastructure?

A. Recommend the use of disk mirroring.

B. Review the adequacy of offsite storage.

C. Review the capacity management process.

D. Recommend the use of a compression algorithm.

When an IS auditor observes the continuous addition of storage resources in the IT infrastructure, reviewing the capacity management process is essential. This action facilitates the understanding of how effectively the organization is managing its resources, ensuring that storage is used efficiently and aligned with current and future needs. Capacity management involves monitoring and evaluating current usage patterns, forecasting future needs, and implementing policies and procedures to optimize resource utilization. By focusing on the capacity management process, the auditor can identify whether the ongoing increase in storage is a response to growing data needs, inefficiencies, or potentially unregulated growth. This insight can lead to improved strategies for resources allocation, cost management, and performance optimization, ensuring that the IT infrastructure remains responsive to the organization's requirements. In contrast, the other options, while they may have relevance in specific contexts, do not directly address the underlying reason behind the continuous addition of storage. For instance, recommending disk mirroring focuses on data redundancy rather than addressing capacity management directly. Similarly, reviewing offsite storage adequacy pertains to backup strategies rather than the efficiency of current capacity utilization. Finally, suggesting a compression algorithm may help with space savings but does not resolve the fundamental capacity management issues or strategic planning associated with resource allocation.

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://cisadomain4.examzify.com

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