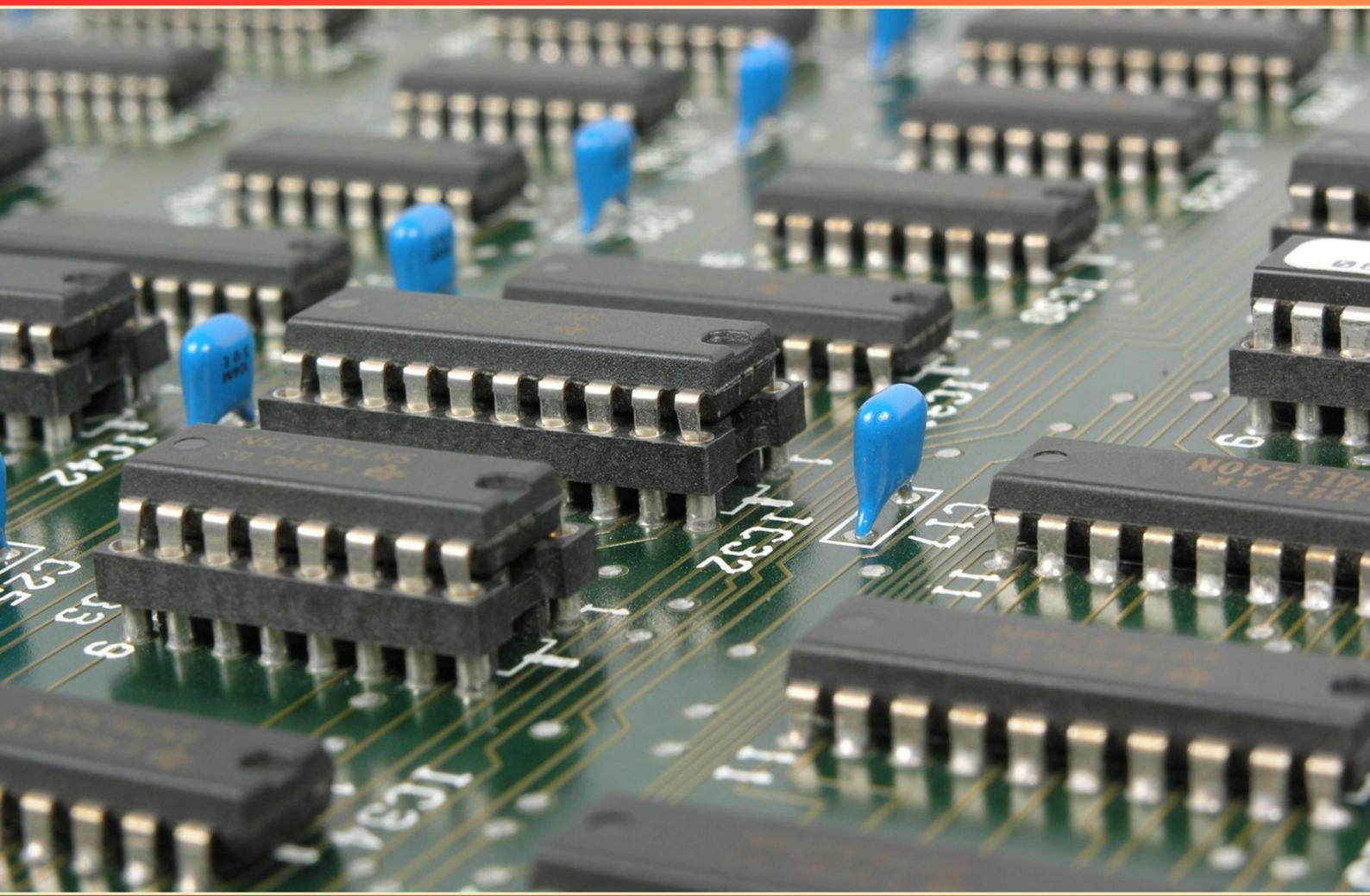
INFORMATION SYSTEMS AND CONTROLS (ISC) CPA PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://isccpa.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 is the purpose of an Access Control List (ACL)?

A. To monitor network traffic

B. To perform log analysis

C. To outline user permissions for accessing resources

D. To detect unauthorized intrusions

2. Which of the following is a primary component of the NIST Privacy Framework?

A. Control: management structure

B. Monitor: tracking compliance

C. Assess: evaluating software solutions

D. Audit: verifying financial transactions

3. Which management objective covers the organization of resources for effective technology use?

A. APO

B. BAI

C. DSS

D. MEA

4. Which item should be described in the management's description of the system?

A. Size of the organization

B. Types of services provided

C. Company financials

D. Number of employees

5. What is one requirement under “Maintain a Vulnerability Management Program” in PCI DSS?

A. Encrypt transaction data across public networks

B. Identify and authenticate access to the system

C. Protect systems against malware and regularly update anti-virus software

D. Regularly monitor and test network access

SAMPLE

6. What happens to the purchase order after the receiving department enters the quantity received?

A. It is closed and updated in the inventory sub ledger

B. It is sent for approval to managers

C. It is filed for audit purposes

D. It is forwarded to HR for records

7. Which trust service is often analyzed during risk management planning?

A. Security

B. Processing Integrity

C. Privacy

D. Availability

8. What type of DLP system is focused on preventing data transfer from cloud services?

A. Network-Based DLP

B. Cloud-Based DLP

C. Hybrid DLP

D. Endpoint-Based DLP

9. What is the main purpose of the NIST framework profiles?

A. To measure cybersecurity risk and provide guidelines for IT management

B. To define data privacy regulations for organizations

C. To outline the steps for implementing new software

D. To enhance workforce productivity

10. Which type of attack relies on creating false communications to impersonate legitimate users?

A. Address Resolution Spoofing

B. Mobile Code Attack

C. Timing Attack

D. Reverse Shell Attack

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the purpose of an Access Control List (ACL)?

A. To monitor network traffic

B. To perform log analysis

C. To outline user permissions for accessing resources

D. To detect unauthorized intrusions

An Access Control List (ACL) serves to outline user permissions for accessing resources within a computing environment. This mechanism acts as a set of rules that determines what users or systems can do with various resources, such as files or network routers. By specifying permissions related to actions such as reading, writing, or executing files, an ACL helps enforce security policies and ensures that only authorized users can access certain data or perform specific functions. The significance of ACLs extends to varying environments, including file systems, networks, and applications, where they play a critical role in safeguarding sensitive information and maintaining compliance with security standards. The clarity in specifying user rights is vital in preventing unauthorized access and ensuring that users can perform their duties without overreaching permissions. The other options address distinct functionalities that do not align with the primary purpose of ACLs. Monitoring network traffic pertains to assessing the flow of data through networks, while log analysis involves reviewing logs for insights such as troubleshooting or auditing. Detecting unauthorized intrusions typically relies on intrusion detection systems or similar technologies, rather than access control mechanisms like ACLs.

2. Which of the following is a primary component of the NIST Privacy Framework?

A. Control: management structure

B. Monitor: tracking compliance

C. Assess: evaluating software solutions

D. Audit: verifying financial transactions

The primary component of the NIST Privacy Framework is the management structure, which emphasizes the importance of governance in privacy risk management. This framework is designed to help organizations manage privacy risks in a comprehensive and structured way. The management structure component addresses how an organization can lead and govern its privacy efforts, ensuring accountability and the establishment of roles and responsibilities related to privacy practices. While other aspects such as monitoring compliance, evaluating software solutions, and auditing financial transactions play roles in a broader context of organizational privacy management and risk assessment, they do not encapsulate the foundational governance principles outlined in the NIST Privacy Framework. The framework is structured to guide an organization in not only defining its approach to privacy but also in fostering a culture where privacy is prioritized and effectively managed at all levels of the organization. This focus on a strong management structure helps in aligning privacy efforts with overall business objectives and regulatory requirements.

SAMPLE

3. Which management objective covers the organization of resources for effective technology use?

A. APO

B. BAI

C. DSS

D. MEA

The correct answer is associated with the APO (Align, Plan, and Organize) objective within the context of information systems and controls. This objective focuses on ensuring that an organization's resources are effectively organized and managed to support the use of technology. It emphasizes strategic alignment of IT with the business goals, allowing organizations to maximize their resources and optimize technology utilization. In detail, APO involves planning and designing IT management systems that support a company's strategies and objectives. This includes establishing the necessary structures, processes, and capabilities to ensure that technology integrates seamlessly with overall business operations. It aims to ensure that adequate resources—such as people, processes, and technology—are in place to achieve the desired outcomes. By prioritizing the organization and alignment of resources, APO serves as a foundational element in the effective utilization of technology to meet an organization's goals. This ensures that technology is not only deployed but is also strategically managed to drive efficiency and effectiveness.

4. Which item should be described in the management's description of the system?

A. Size of the organization

B. Types of services provided

C. Company financials

D. Number of employees

The management's description of the system is crucial for providing stakeholders with a clear understanding of how the organization operates, the context of its systems, and the nature of its services. Describing the types of services provided is essential because it directly informs stakeholders about the core functions and offerings of the entity. Understanding the types of services is vital as it frames the operational context and helps in assessing the efficiency, effectiveness, and risks associated with those services. This description serves as a foundation for analyzing the systems and controls in place, ensuring that they are tailored to support and enhance service delivery. While the size of the organization, company financials, and number of employees may provide relevant background information, they do not specifically inform about the operational framework and functionality of the systems in place as effectively as the types of services provided. The services definition helps in understanding the primary focus of the organization and provides critical insights into the systems that support those operations.

SAMPLE

5. What is one requirement under “Maintain a Vulnerability Management Program" in PCI DSS?

A. Encrypt transaction data across public networks

B. Identify and authenticate access to the system

C. Protect systems against malware and regularly update anti-virus software

D. Regularly monitor and test network access

The "Maintain a Vulnerability Management Program" requirement in the PCI DSS emphasizes the importance of protecting systems against vulnerabilities that could be exploited by attackers. Choosing the option that mentions protecting systems against malware and regularly updating anti-virus software directly aligns with this requirement because it addresses the necessity of having defensive measures in place against malware, which is a critical aspect of maintaining system integrity and security. By implementing anti-malware solutions and ensuring they are kept up-to-date, organizations can effectively reduce the risk of malware infections that could lead to unauthorized access to sensitive cardholder data. Regular updates to anti-virus software are essential in providing the latest protection against newly discovered threats, ensuring that systems remain secure over time. Other options, while important aspects of PCI DSS compliance, do not specifically relate to maintaining vulnerability management. For instance, encrypting transaction data is crucial for protecting data in transit but does not directly pertain to vulnerability management. Similarly, identifying and authenticating access, while essential for overall security, focuses more on access control than on actively managing vulnerabilities. Lastly, monitoring and testing network access are also important for security but are broader measures not specifically tied to the vulnerability management program outlined in the standard.

6. What happens to the purchase order after the receiving department enters the quantity received?

A. It is closed and updated in the inventory sub ledger

B. It is sent for approval to managers

C. It is filed for audit purposes

D. It is forwarded to HR for records

When the receiving department enters the quantity received, the purchase order is typically closed and updated in the inventory sub ledger. This reflects the completion of the transaction, indicating that the ordered items have been received in the appropriate quantities. Closing the purchase order in the system is essential for maintaining accurate inventory records and helps in financial reporting, as it updates the inventory values on hand and ensures that accounts payable can process payments for received goods accurately. The update in the inventory sub ledger is crucial for tracking stock levels and ensuring that accounting records reflect the reality of the inventory status, which aids in decision-making, planning, and further purchasing. This process supports effective inventory management and helps prevent discrepancies that could arise from untracked or unrecorded stock movements. The other options do not accurately represent the standard procedure following the receipt of goods. Approval processes typically occur prior to the receipt, filing for audit purposes is generally a separate activity that does not directly involve the status of the purchase order once the items are received, and forwarding records to HR is not relevant to the inventory or purchasing process.

SAMPLE

7. Which trust service is often analyzed during risk management planning?

A. Security

B. Processing Integrity

C. Privacy

D. Availability

The trust service that is often analyzed during risk management planning is security. In the context of risk management, security refers to the protection of information systems against unauthorized access, breaches, and threats that may compromise the integrity, confidentiality, or availability of data. During risk management planning, organizations assess various threats and vulnerabilities to their information systems and data. A key component of this process involves implementing security measures to mitigate risks associated with potential attacks or breaches. It includes evaluating policies, procedures, and technical safeguards that protect information systems from both external and internal threats. Incorporating security into risk management ensures that an organization not only understands its exposure to risks but also implements appropriate controls and resources to protect sensitive information effectively. This focus on security is foundational as it lays the groundwork for ensuring the reliability of other trust services, such as processing integrity, privacy, and availability, all of which can be influenced by the effectiveness of security measures in place.

8. What type of DLP system is focused on preventing data transfer from cloud services?

A. Network-Based DLP

B. Cloud-Based DLP

C. Hybrid DLP

D. Endpoint-Based DLP

The focus of a Cloud-Based Data Loss Prevention (DLP) system is explicitly on preventing unauthorized data transfer from cloud services. This type of DLP solution is designed to monitor and protect sensitive information that is stored, used, or transmitted in cloud applications. Given the increasing reliance on cloud services for data storage and processing, a Cloud-Based DLP system implements controls to ensure that sensitive data is not improperly accessed or transmitted outside of the organization's configured policies. This system can effectively analyze user activities, apply data categorization, and enforce security policies specific to cloud environments, ensuring that data is adequately protected against breaches and unintentional leakage. It integrates with cloud services, providing visibility and control over data usage and transfers occurring in the cloud. In contrast, other types of DLP systems may not specifically focus on cloud environments. For instance, Network-Based DLP solutions monitor and control data transfers across the network, but they might not specifically address cloud service interactions. Hybrid DLP combines elements of various types, but it does not specifically emphasize cloud service communications. Endpoint-Based DLP systems focus on protecting data stored on individual devices such as laptops or desktops, thus lacking the focused capability to manage cloud-related data transfers effectively. Therefore, the specificity of Cloud-Based D

SAMPLE

9. What is the main purpose of the NIST framework profiles?

A. To measure cybersecurity risk and provide guidelines for IT management

B. To define data privacy regulations for organizations

C. To outline the steps for implementing new software

D. To enhance workforce productivity

The main purpose of the NIST framework profiles is indeed to measure cybersecurity risk and provide guidelines for IT management. The NIST Cybersecurity Framework offers a systematic approach to managing and reducing cybersecurity risks. It helps organizations to understand their current cybersecurity posture, identify areas for improvement, and set goals for their cybersecurity efforts based on specific needs and requirements. The framework profiles serve as a tool to translate high-level cybersecurity objectives into specific outcomes that organizations can strive toward. By defining these profiles, organizations can align their cybersecurity practices with their overall risk management strategy, thus enhancing their resilience against threats. This structured approach is invaluable for guiding IT management in making informed decisions concerning security investments and practices. In contrast, other options like defining data privacy regulations, outlining steps for software implementation, or enhancing workforce productivity do not directly relate to the primary function of the NIST framework profiles, which is focused on cybersecurity risk management.

10. Which type of attack relies on creating false communications to impersonate legitimate users?

A. Address Resolution Spoofing

B. Mobile Code Attack

C. Timing Attack

D. Reverse Shell Attack

The type of attack that involves creating false communications to impersonate legitimate users is Address Resolution Spoofing. This attack exploits the Address Resolution Protocol (ARP), which is used to map network addresses (like IP addresses) to physical addresses (like MAC addresses) in a local area network. By sending forged ARP replies that associate the attacker's MAC address with a legitimate IP address, the attacker can impersonate a legitimate user or device on the network. This can lead to various malicious activities, such as intercepting data intended for the legitimate user, conducting man-in-the-middle attacks, or causing denial-of-service conditions. The essence of this attack lies in its ability to deceive other network nodes into thinking that the attacker is a trusted participant, allowing for unauthorized access to sensitive information or resources. The other types of attacks mentioned do not primarily rely on impersonation through false communications. A Mobile Code Attack typically refers to executing code that can change the behavior of systems, often used in web environments. A Timing Attack is focused on measuring the time taken for certain operations to infer sensitive information. A Reverse Shell Attack involves an attacker gaining remote access to a user's machine by establishing a connection back to the attacker's system, which is not about impersonating legitimate users through

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://isccpa.examzify.com

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

SAMPLE