ASSOCIATE QUALIFIED SECURITY ASSESSOR (AQSA) CERTIFICATION PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://qualityassessoraqsa.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. **According to PCI DSS requirement 1.2, firewall and router configurations must restrict connections between which two entities?**

   A. Internet and corporate networks

   B. Corporate networks and the cardholder data environment

   C. Cardholder data environment and payment processors

   D. Corporate networks and external vendors

2. **Which logs need to be reviewed at least daily?**

   A. All email logs

   B. Logs of security events and systems storing, processing, or transmitting CHD and/or SAD

   C. Only application logs

   D. Visitor access logs

3. **What is the primary role of the PCI SSC?**

   A. To enforce payment card regulations

   B. To provide oversight of Payment Card Industry Data Security Standards

   C. To validate Payment Card Industry service providers

   D. To set prices for payment processing services

4. **Which device is NOT typically involved in establishing network segmentation controls?**

   A. Firewalls

   B. Switched networks

   C. Physical storage devices

   D. Routers

5. **What does SAQ-B indicate for merchants?**

   A. Use of mobile payment applications only

   B. Use of electronic cardholder data storage

   C. Use of imprint machines or standalone dial-out terminals

   D. Full control over cardholder data processing

SAMPLE

6. Which role plays a critical part in the oversight of PCI DSS compliance?

A. Network Administrator

B. Executive Management

C. Security Technician

D. External Auditor

7. What does the term "split knowledge" refer to in the context of security measures?

A. A method where multiple people share the same key

B. Each person knowing only their own component of a key

C. A single person having access to the entire key

D. Using a single password for all users

8. A secure network should not expose what type of data?

A. Transactional data

B. Cardholder data

C. Operational data

D. Employee data

9. Which aspect does PCI PTS primarily address?

A. Tamper detection in card manufacturing

B. Cryptographic processes for PIN protection

C. Secure card personalization processes

D. Encryption of remote payment communications

10. What is required for stateful firewalls regarding connections into the Cardholder Data Environment (CDE)?

A. Optional

B. Not necessary

C. Required

D. Prohibited

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. According to PCI DSS requirement 1.2, firewall and router configurations must restrict connections between which two entities?

A. Internet and corporate networks

B. Corporate networks and the cardholder data environment

C. Cardholder data environment and payment processors

D. Corporate networks and external vendors

The requirement described is focused on the protection of cardholder data within the context of the Payment Card Industry Data Security Standard (PCI DSS). One of the critical aspects of creating and maintaining a secure environment involves establishing strict controls around where and how cardholder data can be accessed. In this case, option B correctly identifies the need to restrict connections between corporate networks and the cardholder data environment. The rationale for this specific requirement is to mitigate the risks associated with unauthorized access to cardholder data. By limiting the communication pathways between these two environments, organizations can significantly reduce the potential attack surface that cybercriminals may exploit. The cardholder data environment (CDE) contains sensitive information such as credit card numbers and personal data. Thus, it is imperative that access to this environment be controlled tightly to prevent data breaches or leakage. Other choices do not capture the specific focus on safeguarding the cardholder data environment as required by PCI DSS. While connections between the internet and corporate networks, or external vendors and corporate networks, are important considerations for overall network security, the primary emphasis of PCI DSS requirement 1.2 is on protecting the cardholder data environment itself from the corporate network, ensuring that only authorized and necessary connections are allowed.

2. Which logs need to be reviewed at least daily?

A. All email logs

B. Logs of security events and systems storing, processing, or transmitting CHD and/or SAD

C. Only application logs

D. Visitor access logs

The requirement to review logs at least daily is critical for maintaining the security and integrity of systems that handle sensitive information, such as Cardholder Data (CHD) and Sensitive Authentication Data (SAD). Reviewing logs from systems that store, process, or transmit CHD and SAD helps detect and respond to suspicious activities or breaches in real-time. Daily review of these logs is crucial because it allows organizations to identify anomalies or unauthorized access attempts that could jeopardize sensitive information. By actively monitoring these logs, security teams can quickly mitigate risks, ensure compliance with security standards, and protect sensitive data from potential threats. While email logs, application logs, and visitor access logs serve important functions in overall security and auditing, the logs specifically linked to systems handling CHD and SAD are emphasized due to their connection to financial transactions and the inherent risks associated with such data. Therefore, focusing on those logs helps organizations prioritize their security efforts more effectively.

SAMPLE

3. What is the primary role of the PCI SSC?

A. To enforce payment card regulations

B. To provide oversight of Payment Card Industry Data Security Standards

C. To validate Payment Card Industry service providers

D. To set prices for payment processing services

The primary role of the PCI Security Standards Council (PCI SSC) is to provide oversight of the Payment Card Industry Data Security Standards (PCI DSS). This involves the creation, management, and ongoing development of security standards designed to protect cardholder data. The PCI SSC collaborates with various stakeholders in the payment card industry, including merchants, financial institutions, and card brands, to ensure that the standards remain effective and relevant in a rapidly changing technological and threat landscape. By overseeing the development of these standards, the PCI SSC ensures that organizations that handle cardholder data are implementing adequate security measures to help protect against data breaches and fraud. This focus on providing oversight is crucial because it helps to maintain a baseline level of security across the industry, promoting trust and safety in payment card transactions. Other options relate to aspects that may involve the PCI SSC but do not capture its primary role as effectively as the correct choice does. For example, while enforcing payment card regulations is important, the council does not have the authority to enforce regulations; it provides guidance and standards instead. Validation of service providers and setting prices for payment processing services are external activities related to the industry, but they do not define the core mission of the PCI SSC, which is centered on standard development and oversight.

4. Which device is NOT typically involved in establishing network segmentation controls?

A. Firewalls

B. Switched networks

C. Physical storage devices

D. Routers

Network segmentation controls are primarily about dividing a network into smaller, manageable sections to enhance security and performance. Devices that are part of this process typically include firewalls, routers, and switches, as they are configured to control traffic, enforce policies, and route data correctly between different segments. Firewalls are crucial for monitoring and controlling incoming and outgoing network traffic based on predetermined security rules, effectively acting as a barrier between trusted internal networks and untrusted external networks. Routers can segment networks by directing traffic and can implement rules to manage data flow between different network segments, often utilizing access control lists. Switched networks involve devices called switches that connect devices within the same network segment, enabling efficient data transfer and reducing broadcast traffic across the entire network. By controlling which devices can communicate with each other, switches play a key role in network segmentation. On the other hand, physical storage devices, while important for data storage and management, do not play a direct role in the implementation of network segmentation controls. Their purpose is primarily to store data rather than manage or control network traffic or enforce policies that would segment networks. Therefore, among the given options, physical storage devices stand out as not typically involved in establishing network segmentation controls.

SAMPLE

5. What does SAQ-B indicate for merchants?

A. Use of mobile payment applications only

B. Use of electronic cardholder data storage

C. Use of imprint machines or standalone dial-out terminals

D. Full control over cardholder data processing

SAQ-B (Self-Assessment Questionnaire B) is specifically designed for merchants who process cardholder data only through standalone terminals that are not connected to the internet. This means that these merchants do not store cardholder data electronically nor do they use custom applications for processing payments. The correct association with SAQ-B is that it pertains to merchants who utilize imprint machines or standalone dial-out terminals. This setup indicates a level of security that aligns with regulatory compliance, as these methods limit the risk of exposure to electronic cardholder data. Merchants using such terminals are only handling card data in a way that minimizes their technological vulnerability. The other choices describe scenarios that do not align with the requirements of SAQ-B. The use of mobile payment applications or electronic cardholder data storage would imply a more complex operating environment that necessitates a different self-assessment questionnaire. Furthermore, having full control over cardholder data processing would extend beyond the simplified requirements laid out for those eligible for SAQ-B.

6. Which role plays a critical part in the oversight of PCI DSS compliance?

A. Network Administrator

B. Executive Management

C. Security Technician

D. External Auditor

Executive Management plays a critical role in the oversight of PCI DSS compliance because they hold the ultimate responsibility for the organization's security policies and practices. Their involvement is essential to ensure that adequate resources, including funding and personnel, are allocated toward achieving and maintaining compliance with PCI DSS requirements. By setting the tone at the top, Executive Management can foster a security-aware culture throughout the organization, motivating all employees to recognize the importance of data security and compliance. Additionally, Executive Management is responsible for approving policies and procedures, ensuring that compliance efforts align with the business goals, and addressing any identified vulnerabilities or risks. They must also engage with various stakeholders, ensuring everyone from IT to finance understands their role in maintaining compliance and protecting cardholder data. This oversight is crucial because, without proper direction and support from upper management, compliance initiatives may lack the necessary commitment, resources, and authority to be effective in safeguarding sensitive information.

SAMPLE

7. What does the term "split knowledge" refer to in the context of security measures?

A. A method where multiple people share the same key

B. Each person knowing only their own component of a key

C. A single person having access to the entire key

D. Using a single password for all users

The term "split knowledge" refers to a security measure in which no single individual has access to the complete key or sensitive information required to perform a particular function or task. In this context, each person is only aware of a specific component or portion of the key, ensuring that the full key cannot be reconstructed or misused by any single individual. This approach is essential for enhancing security, as it creates a barrier against potential insider threats and reduces the risk of unauthorized access. By requiring cooperation among multiple individuals to access the complete information, organizations can improve the overall security posture and protect sensitive data more effectively. Other approaches, such as sharing a single key among multiple people or allowing a single person full access to the entire key, do not provide the same level of security and could potentially lead to vulnerabilities. Using a single password for all users also undermines the principle of split knowledge, as it can easily be shared or compromised by any user with access.

8. A secure network should not expose what type of data?

A. Transactional data

B. Cardholder data

C. Operational data

D. Employee data

The exposure of cardholder data poses significant risks, particularly in the context of security and compliance regulations such as the Payment Card Industry Data Security Standard (PCI DSS). This type of data includes sensitive information like credit card numbers, expiration dates, and security codes, which, if compromised, can lead to fraud and identity theft. Therefore, a secure network must implement robust security measures to protect cardholder data, ensuring that it is encrypted during transmission and stored securely. The potential for financial loss and legal ramifications for organizations that fail to safeguard this information underscores the importance of maintaining the confidentiality and integrity of cardholder data in a secure network environment. Transactional, operational, and employee data also require protection, but they do not carry the same level of risk or regulatory pressure associated with cardholder data. Thus, the primary focus of a secure network should prioritize preventing the exposure of cardholder data to mitigate these serious threats.

SAMPLE

9. Which aspect does PCI PTS primarily address?

A. Tamper detection in card manufacturing

B. Cryptographic processes for PIN protection

C. Secure card personalization processes

D. Encryption of remote payment communications

PCI PTS (Payment Card Industry PIN Transaction Security) primarily focuses on the security of PIN-based payment transactions, particularly emphasizing cryptographic processes for the protection of Personal Identification Numbers (PINs). The standard outlines requirements for the secure management, storage, and cryptography applied to PINs as they are entered by cardholders at payment terminals. By focusing on cryptographic processes, PCI PTS ensures that PINs remain confidential and secure during the transaction process. This includes guidelines on how PINs should be encrypted during entry and transmission, protecting them from potential eavesdropping or tampering by malicious actors. Compliance with these standards is critical for maintaining the integrity and security of payment processing systems that handle PIN transactions. The other aspects mentioned, such as tamper detection in card manufacturing, secure card personalization processes, and encryption of remote payment communications, fall under different PCI security standards or guidelines, making them important but not specifically addressed by PCI PTS.

10. What is required for stateful firewalls regarding connections into the Cardholder Data Environment (CDE)?

A. Optional

B. Not necessary

C. Required

D. Prohibited

Stateful firewalls play a crucial role in protecting the Cardholder Data Environment (CDE) by monitoring and controlling the inbound and outbound traffic based on the state of active connections. For connections into the CDE, it is essential for stateful firewalls to be implemented as they provide a higher level of security compared to stateless firewalls. By maintaining a table of active connections, stateful firewalls can effectively track ongoing sessions and apply specific rules to allow or deny traffic based on the context of that traffic, greatly reducing the risk of unauthorized access. This capability is particularly important in a CDE, which needs to be secured against various threats, as it contains sensitive cardholder information. The requirement for stateful firewalls within the CDE is in line with best practices for protecting payment systems and compliance with security standards, which emphasize the necessity to verify and manage all connections to sensitive environments. This proactive management of data flows is key to maintaining the integrity and confidentiality of cardholder data.

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://qualityassessoraqsa.examzify.com

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

SAMPLE