ISA/IEC 62443 CYBERSECURITY FUNDAMENTALS SPECIALIST (IC32) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://isaiec62443ic32.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. **Which of the following is NOT one of the threats identified by the DAMIT mnemonic?**

   A. Unauthorized Access

   B. Malware

   C. Theft of Assets

   D. Denial of Service (DoS)

2. **Which layer does the Data Link Protocol operate in the OSI model?**

   A. Layer 1

   B. Layer 2

   C. Layer 3

   D. Layer 4

3. **What does SDLC stand for in networking?**

   A. Synchronous Data Link Control

   B. Synchronous Data Layer Control

   C. Serial Data Link Control

   D. Sequential Data Link Control

4. **What does a firewall policy ACL rule typically include?**

   A. Encryption methods and protocols

   B. Source and destination IP addresses

   C. Authorized personnel list

   D. Network bandwidth limits

5. **Which protocol is known as the Routing Information Protocol?**

   A. IPX

   B. RIP

   C. OSPF

   D. BGP

SAMPLE

6. Which of the following is not classified as a routable protocol in OSI Layer 3?

A. IPv4

B. ICMP

C. HTTP

D. IPSec

7. What type of threat agent can be categorized as a natural disaster?

A. Outsider

B. Insider

C. Natural

D. Deliberate actor

8. Which year was the Modbus protocol developed?

A. 1980

B. 1979

C. 1985

D. 1975

9. What are the two main categories of threat sources?

A. Internal and external

B. Only internal and natural

C. Superficial and deep

D. Only deliberate and opportunistic

10. Which of the following is NOT a wireless access technology?

A. Bluetooth (802.15.1)

B. USB 3.0

C. 802.11x

D. Zigbee (802.15.4)

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which of the following is NOT one of the threats identified by the DAMIT mnemonic?

A. Unauthorized Access

B. Malware

C. Theft of Assets

D. Denial of Service (DoS)

*The DAMIT mnemonic is designed to capture various cybersecurity threats in the context of industrial control systems. The elements encapsulated by DAMIT include **Denial of Service (DoS)**, **Unauthorized Access**, and **Malware**. Each of these threats can significantly impact the confidentiality, integrity, and availability of systems in an industrial setting. The mention of **Theft of Assets** is not part of the DAMIT acronym. While theft of assets can certainly be a concern within the broader scope of cybersecurity, it does not fall under the specific threats identified by DAMIT. This mnemonic is focused on immediate threats that can be classified and understood within the framework of cybersecurity risks, whereas asset theft is generally considered a consequence of successful exploitation rather than an immediate threat category. Understanding these categories helps security professionals prioritize their defenses against the specific types of threats they are most likely to encounter, enabling them to develop appropriate strategies and measures.*

2. Which layer does the Data Link Protocol operate in the OSI model?

A. Layer 1

B. Layer 2

C. Layer 3

D. Layer 4

The Data Link Protocol operates at Layer 2 of the OSI model. This layer is responsible for node-to-node data transfer and provides the means for reliable data transfer over a physical link. It handles error detection and correction (to some extent), controls how data is placed and received from the medium, and addresses hardware addresses—essentially managing communication between devices on the same local network. This capability is fundamental for both wired and wireless communication. Layer 2 ensures that the data frames are formatted correctly and that they can communicate effectively across the physical network, which is managed by Layer 1, but that layer does not provide the formatting or protocol-level functionality required for effective communication; those responsibilities lie with Layer 2. In contrast, Layers 1, 3, and 4 have distinct functionalities—Layer 1 deals with the physical aspects of the network, such as cables and signals; Layer 3 focuses on the network-layer routing and logical addressing; and Layer 4 provides transport-layer services, including end-to-end communication and flow control. Each layer has a specific set of responsibilities, and understanding these helps clarify the role of the Data Link Protocol in the OSI model. Thus, identifying Layer 2 as the correct answer signifies recognizing its critical

SAMPLE

3. What does SDLC stand for in networking?

A. Synchronous Data Link Control

B. Synchronous Data Layer Control

C. Serial Data Link Control

D. Sequential Data Link Control

SDLC stands for Synchronous Data Link Control. This is a protocol used in data communications and networking to manage the flow of data between computers. SDLC is particularly important in scenarios where multiple devices are connected and need to communicate effectively without data loss or corruption. It operates in a synchronous manner, meaning it uses timing signals to ensure that the sending and receiving systems are aligned in their communication. The choice represents a widely used method for controlling data transmission and ensuring reliable delivery over communication links. SDLC allows for both error checking and data framing, making it a fundamental component in various networking protocols. In contrast, the other options present variations of the term but do not accurately represent the standard acronym recognized within networking contexts.

4. What does a firewall policy ACL rule typically include?

A. Encryption methods and protocols

B. Source and destination IP addresses

C. Authorized personnel list

D. Network bandwidth limits

A firewall policy Access Control List (ACL) rule is primarily designed to specify what traffic is allowed or denied through the firewall based on specific criteria. The inclusion of source and destination IP addresses is foundational for defining these rules, as firewall ACLs function by evaluating packets against these address criteria to determine whether to allow or block the traffic. By specifying source and destination IP addresses, a firewall can effectively control the flow of data between different segments of a network or between a network and external sources. This mechanism ensures that only traffic from authorized sources to permitted destinations is permitted, thereby enhancing the security posture of the network. Other options like encryption methods and protocols, authorized personnel lists, and network bandwidth limits do not typically form part of the basic firewall policy ACL rule structure. While encryption methods and protocols might be relevant to the overall security framework of a network, they do not directly dictate the operation of an ACL rule. Authorized personnel lists pertain to user access control rather than the technical specification of traffic handling in context to firewalls. Network bandwidth limits are related to Quality of Service (QoS) policies rather than access control, which focuses specifically on managing and regulating data traffic based on IP addresses.

SAMPLE

5. Which protocol is known as the Routing Information Protocol?

A. IPX

B. RIP

C. OSPF

D. BGP

The Routing Information Protocol, or RIP, is a distance-vector routing protocol used to determine the best route for data packets within an IP network. It employs a simple metric, specifically the hop count, which limits the number of allowable hops to 15. This makes RIP suitable for smaller networks. RIP operates by having routers share their routing tables with neighboring routers at regular intervals, allowing them to update their knowledge of the network topology. This protocol is established in the early days of networking, making it one of the oldest routing protocols still in use, often in simpler implementations where the overhead of more complex protocols is unnecessary. The other protocols listed serve different functions or are used in different contexts within routing. For instance, IPX is associated with Novell's networking architecture rather than IP routing. OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol) are both more advanced routing protocols designed for larger or more complex networks, focusing on scalability and efficiency. OSPF employs a link-state approach while BGP manages the routing between autonomous systems on the internet.

6. Which of the following is not classified as a routable protocol in OSI Layer 3?

A. IPv4

B. ICMP

C. HTTP

D. IPSec

In the context of network protocols, routable protocols are those that can be routed through different networks based on their IP addresses, thus operating at OSI Layer 3 (The Network Layer). The primary function of Layer 3 is to manage device addressing, track the location of devices on the network, and determine the best way to move data. The correct answer, HTTP, is a protocol that operates at OSI Layer 7 (The Application Layer). It is primarily responsible for allowing web servers and clients to communicate by transferring hypertext documents and does not inherently support routing of packets across networks. In contrast, IPv4 is a fundamental network-layer protocol used for addressing and routing packets. ICMP operates at Layer 3, often used for error messages and operational queries. IPSec provides secure network communications by securing IP packets at the network layer but is still classified under Layer 3 protocols since it deals with IP traffic. By recognizing where each protocol operates in the OSI model, you can see why HTTP is not classified as a routable protocol at Layer 3, focusing instead on application-level tasks.

SAMPLE

7. What type of threat agent can be categorized as a natural disaster?

A. Outsider

B. Insider

C. Natural

D. Deliberate actor

The correct answer is natural. This category refers specifically to threat agents that arise from natural events, such as earthquakes, floods, hurricanes, and other environmental phenomena. Unlike the others, which involve human actors, natural threats are uncontrollable events that can cause significant disruption or damage to systems and facilities, including those involved in cybersecurity. The outsider and insider categories involve human behavior, where outsiders typically represent untrusted individuals or entities attempting to breach a system, and insiders are trusted personnel who may compromise the system intentionally or unintentionally. Deliberate actors also involve human agency, focusing on individuals or groups with malicious intent aiming to harm systems or organizations. By recognizing natural disasters as a distinct category of threat, organizations can formulate specific response and mitigation strategies to integrate into their cybersecurity and risk management plans.

8. Which year was the Modbus protocol developed?

A. 1980

B. 1979

C. 1985

D. 1975

The Modbus protocol was developed in 1979, making that the correct answer. Initially created by Modicon to facilitate communication among their programmable logic controllers (PLCs), Modbus was designed to be an open and simple communication protocol that could be utilized on a wide range of devices. Its significance lies in its ability to provide a standard, easy-to-implement methodology that has had a lasting impact on industrial automation and communication systems. The implementation of Modbus has played a crucial role in the interoperability of devices from different manufacturers within industrial environments, contributing to more efficient operations.

9. What are the two main categories of threat sources?

A. Internal and external

B. Only internal and natural

C. Superficial and deep

D. Only deliberate and opportunistic

The two main categories of threat sources are internal and external. This classification is vital in cybersecurity as it helps organizations understand where potential risks and vulnerabilities may originate. Internal threats come from within the organization and can involve employees, contractors, or other insiders who may misuse their access to data or systems, either intentionally or inadvertently. These threats can stem from a lack of awareness, disgruntlement, or accidental actions that compromise security. External threats, on the other hand, originate outside the organization. They can come from a variety of actors, including hackers, rival companies, or nation-states, who seek to exploit vulnerabilities for malicious purposes such as theft, sabotage, or espionage. Understanding both internal and external sources of threats allows organizations to implement comprehensive security strategies to mitigate risks. The other options do not reflect the broad spectrum needed to effectively classify threat sources. Limiting categories to only natural or deliberate sources fails to capture the full range of threats an organization faces, while superficial and deep or only focusing on specific intent misses the holistic view necessary for effective cybersecurity management.

SAMPLE

10. Which of the following is NOT a wireless access technology?

A. Bluetooth (802.15.1)

B. USB 3.0

C. 802.11x

D. Zigbee (802.15.4)

The correct choice is USB 3.0 because it is a wired communication standard rather than a wireless access technology. USB (Universal Serial Bus) is designed for connecting devices to a host computer through physical cables, enabling direct communication and power transfer. It is widely used for various peripherals such as keyboards, mice, and external storage devices. In contrast, Bluetooth, 802.11x (which refers to Wi-Fi standards), and Zigbee are all technologies that enable wireless communication. Bluetooth (802.15.1) facilitates short-range data exchange between devices, 802.11x covers multiple Wi-Fi standards for local area networking, and Zigbee (802.15.4) focuses on low-power, low-data rate wireless communication, particularly for application areas like home automation and industrial control.

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://isaiec62443ic32.examzify.com

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

SAMPLE