WESTERN GOVERNORS UNIVERSITY (WGU) ITAS6291 D488 CYBERSECURITY ARCHITECTURE AND ENGINEERING PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://wgu-itas6291d488.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

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 main purpose of the OAuth protocol in security architecture?**

   A. A. To provide a secure login form

   B. B. To manage network traffic

   C. C. To enable secure authorization

   D. D. To encrypt sensitive data

2. **Which standard is primarily used to assess cloud service providers for security practices?**

   A. A. STAR

   B. B. PCI DSS

   C. C. GDPR

   D. D. CMMI

3. **A systems administrator wants to enable a setting to make it difficult for buffer overflow attacks to locate the area of memory needed to successfully perform an exploit. What is this called?**

   A. Race condition

   B. TOC (Time of Check)

   C. ASLR (Address Space Layout Randomization)

   D. Data execution protection (DEP)

4. **Which of the following is NOT an example of a benefit provided by a CDN?**

   A. Vertical scalability

   B. Improved customer experience

   C. DDoS protection

   D. Horizontal scalability

5. **Why is it important to adopt the principle of least privilege when securing logs in a central log management system?**

   A. A. To ensure open access to all log data

   B. B. To prevent security misconfigurations and restrict access to sensitive log data

   C. C. To classify critical events more efficiently

   D. D. To comply with legal and regulatory requirements

SAMPLE

6. In quantum computing, what physical properties might represent quantum particle information in a qubit?

A. Momentum or spin

B. Voltage

C. Current

D. Resistance

7. What does a CYOD policy specifically provide to employees?

A. Freedom to choose any personal device.

B. A selection of company-approved devices to choose from.

C. Devices strictly for business purposes only.

D. Responsibility for purchasing their devices.

8. Which protocol is primarily used for securing voice over IP (VoIP) communications?

A. A. HTTPS

B. B. SRTP (Secure Real-time Transport Protocol)

C. C. S/MIME (Secure/Multipurpose Internet Mail Extensions)

D. D. FTPS (File Transfer Protocol Secure)

9. What are the two major components of risk that are essential in understanding its evaluation?

A. Impact, Exploitability

B. Impact, Likelihood

C. Integrity, Likelihood

D. Integrity, Exploitability

10. What arrangement includes forty-two participating states and is designed to prevent the destabilizing accumulation of weaponry and military capabilities?

A. e-Discovery

B. Encryption laws

C. Wassenaar arrangement

D. Export laws

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the main purpose of the OAuth protocol in security architecture?

A. A. To provide a secure login form

B. B. To manage network traffic

C. C. To enable secure authorization

D. D. To encrypt sensitive data

The OAuth protocol serves the primary purpose of enabling secure authorization between applications without exposing user credentials. It allows users to grant third-party applications limited access to their resources (like APIs) without sharing their passwords. This mechanism is essential in scenarios where users wish to access services provided by different platforms while maintaining control over their sensitive information. Through OAuth, a user can authorize an application to access data on their behalf—like posting on social media or retrieving profile information—while keeping their login credentials safe and separate from that application. This separation mitigates the risk of credential theft and is particularly important in today's ecosystem where multiple services interact and collaborate frequently. The other choices, while related to aspects of security or functionality, do not encapsulate the core purpose of OAuth. Secure login forms pertain to authentication, not the authorization that OAuth provides. Managing network traffic is a more general network function that does not specifically relate to OAuth's capabilities. Encrypting sensitive data concerns confidentiality and does not directly describe the role of granting access that is central to OAuth's design.

2. Which standard is primarily used to assess cloud service providers for security practices?

A. A. STAR

B. B. PCI DSS

C. C. GDPR

D. D. CMMI

The standard primarily used to assess cloud service providers for security practices is the Security, Trust & Assurance Registry (STAR). This standard provides a framework for cloud service providers to demonstrate their security practices and compliance through rigorous assessments. It is focused specifically on the cloud context, promoting transparency and accountability in how cloud services protect data and maintain security measures. STAR incorporates principles and controls derived from widely accepted standards, such as ISO 27001, but tailors them to the cloud environment. This focus ensures that organizations using cloud services can evaluate their potential providers based on a recognized and credible benchmark, making informed decisions about security benefits and risks. In contrast, other standards, such as PCI DSS, are primarily focused on payment card data security, and GDPR relates to data protection and privacy, particularly in Europe, rather than specifically addressing cloud service security practices. CMMI is a framework that addresses process improvement rather than specific security assessments. So, STAR being specifically designed for cloud services set it apart as the most relevant standard in this context.

SAMPLE

3. A systems administrator wants to enable a setting to make it difficult for buffer overflow attacks to locate the area of memory needed to successfully perform an exploit. What is this called?

A. Race condition

B. TOC (Time of Check)

C. ASLR (Address Space Layout Randomization)

D. Data execution protection (DEP)

The term that describes the technique used to make it difficult for buffer overflow attacks to pinpoint the necessary area of memory for a successful exploit is Address Space Layout Randomization, commonly abbreviated as ASLR. This security feature randomizes the memory addresses used by a program each time it is executed, which means that the location of key areas, such as the stack, heap, and libraries, is not predictable. By randomizing address spaces, ASLR effectively complicates the attacker's ability to craft effective payloads for buffer overflow exploits. Since the address of the buffer and the location of the executed code change each time the application starts, the attacker cannot reliably leverage a fixed address to execute their malicious code. This increases the difficulty of successful alignment in their attack strategies. Other concepts, such as race conditions, depend on timing and synchronization issues in a system, which is separate from memory address exploitation. The Time of Check, Time of Use (TOC/TOU) attacks pertain to the exploitation of the time gap between checking permissions and using a resource, not specifically to memory layout. Data Execution Protection (DEP) is another security measure that marks certain areas of memory as non-executable, which prevents code from executing in those locations but does not randomize

4. Which of the following is NOT an example of a benefit provided by a CDN?

A. Vertical scalability

B. Improved customer experience

C. DDoS protection

D. Horizontal scalability

Vertical scalability, often referred to as "scaling up," involves adding more resources (such as CPU or RAM) to a single server to handle increased load. This approach can be limiting because it relies on a single machine and can reach a point where it cannot be further upgraded effectively. In contrast, CDNs (Content Delivery Networks) primarily enhance content delivery efficiency and improve site performance by distributing content across multiple edge locations. The benefits provided by a CDN include: - Improved customer experience, achieved through faster content delivery by serving cached content from a location closer to the user. - DDoS protection, which is a critical feature in safeguarding against distributed denial-of-service attacks by absorbing and dispersing excessive traffic across the CDN infrastructure. - Horizontal scalability, which allows adding more servers or nodes to distribute the load and manage spikes in user demand more effectively. Therefore, vertical scalability is not a characteristic benefit of a CDN, as CDNs focus on optimizing content delivery through horizontal scaling methods instead.

SAMPLE

5. Why is it important to adopt the principle of least privilege when securing logs in a central log management system?

A. A. To ensure open access to all log data

B. B. To prevent security misconfigurations and restrict access to sensitive log data

C. C. To classify critical events more efficiently

D. D. To comply with legal and regulatory requirements

Adopting the principle of least privilege is essential in the context of securing logs in a central log management system because it minimizes the risk of unauthorized access and potential misuse of sensitive log data. By restricting access to only those individuals or systems that absolutely need it, organizations can reduce the likelihood of security breaches. This approach also helps to prevent accidental or deliberate alterations or deletions of log data, which are critical for forensic investigations and maintaining the integrity of security monitoring. Restricting permissions in line with the principle of least privilege ensures that only trusted personnel can view or manage sensitive logs. This is particularly important when logs contain information related to security events, user activity, or system changes that could expose vulnerabilities or sensitive data if accessed inappropriately. While compliance with legal and regulatory requirements is important, the primary focus of least privilege is on enhancing security by limiting access. This proactive measure directly contributes to the overall security posture of the organization, making it harder for malicious actors to exploit vulnerabilities related to log management. Thus, the adoption of the least privilege principle is a foundational practice in protecting sensitive information effectively within log management systems.

6. In quantum computing, what physical properties might represent quantum particle information in a qubit?

A. Momentum or spin

B. Voltage

C. Current

D. Resistance

In quantum computing, a qubit (quantum bit) is the fundamental unit of quantum information. It can represent information in ways that classical bits cannot, taking advantage of quantum properties. One of the key features of qubits is their ability to exist in a superposition of states, and this is often realized through specific physical properties of quantum particles. Momentum and spin are properties that directly correlate with quantum mechanical systems and can be utilized to represent the states of qubits. For example, the spin of an electron can be aligned in different directions (such as up or down), and these orientations can represent the binary states of 0 and 1. Similarly, momentum can be used to encode information due to its inherent quantum characteristics. On the other hand, voltage, current, and resistance are primarily classical electrical parameters and do not inherently encapsulate the quantum properties needed for qubits. These parameters can describe classical electronic systems but do not provide the necessary foundation for representing quantum information. Quantum computing relies on the unique aspects of quantum mechanics, such as superposition and entanglement, which are best illustrated through properties like momentum and spin.

SAMPLE

7. What does a CYOD policy specifically provide to employees?

A. Freedom to choose any personal device.

B. A selection of company-approved devices to choose from.

C. Devices strictly for business purposes only.

D. Responsibility for purchasing their devices.

A CYOD policy, which stands for "Choose Your Own Device," allows employees to select from a range of devices that have been approved by the company for work-related purposes. This approach strikes a balance between offering employees some degree of autonomy in selecting their devices while ensuring that those devices meet specific security and operational standards set by the organization. By providing a selection of company-approved devices, the organization can maintain control over the security and management of these devices, ensuring they align with corporate policies and standards. This prevents potential security risks associated with allowing employees to use any device they choose, which may not meet security requirements or could introduce vulnerabilities into the company network. In contrast, a policy that allows complete freedom to choose any personal device might lead to significant security challenges, as not all devices may support adequate security measures or updates. Similarly, having devices strictly for business purposes only would limit employee flexibility and satisfaction. Lastly, placing the responsibility for purchasing devices on employees could create inequities and barriers for some staff, reducing overall workforce morale and effectiveness.

8. Which protocol is primarily used for securing voice over IP (VoIP) communications?

A. A. HTTPS

B. B. SRTP (Secure Real-time Transport Protocol)

C. C. S/MIME (Secure/Multipurpose Internet Mail Extensions)

D. D. FTPS (File Transfer Protocol Secure)

The protocol primarily used for securing voice over IP (VoIP) communications is SRTP (Secure Real-time Transport Protocol). SRTP is specifically designed to provide encryption, message authentication, and integrity, which are essential for maintaining the confidentiality and integrity of voice communications over potentially insecure networks. Voice traffic is sensitive and often transmitted in real-time, making it critical to protect it against eavesdropping and tampering. SRTP addresses these concerns by encrypting the voice packets and ensuring that they are sent securely, providing a much-needed layer of security for VoIP communications. In contrast, other protocols mentioned serve different purposes. HTTPS is focused on securing web traffic, S/MIME is used for securing email messages, and FTPS is for securing file transfers. Consequently, SRTP stands out as the correct choice due to its specific design and function for safeguarding voice communications in the realm of VoIP.

SAMPLE

9. What are the two major components of risk that are essential in understanding its evaluation?

A. Impact, Exploitability

B. Impact, Likelihood

C. Integrity, Likelihood

D. Integrity, Exploitability

The correct pairing of components essential for understanding risk evaluation consists of impact and likelihood. Impact refers to the potential consequences or damage that could result from a security incident or threat, while likelihood indicates the probability that a particular threat may exploit a vulnerability. Evaluating both of these elements is crucial for determining overall risk levels in cybersecurity. Assessing impact allows organizations to prioritize their security efforts based on the severity of potential risks, while understanding likelihood helps to gauge how realistic those risks are in the current environment. Together, these factors create a comprehensive view of risk, enabling informed decision-making regarding resource allocation for protective measures and incident response. In the other options, while integrity and exploitability are important concepts in security contexts, they do not encapsulate the full scope of risk evaluation in the manner that impact and likelihood do. Integrity focuses on the accuracy and trustworthiness of information, while exploitability pertains to how easily a vulnerability can be leveraged by an attacker, but without the context of how likely that event is to occur or how severe the consequences would be, these factors alone do not provide a complete risk assessment.

10. What arrangement includes forty-two participating states and is designed to prevent the destabilizing accumulation of weaponry and military capabilities?

A. e-Discovery

B. Encryption laws

C. Wassenaar arrangement

D. Export laws

The Wassenaar Arrangement is a multilateral export control regime that includes forty-two participating states and aims to prevent the destabilizing accumulation of conventional weapons and military capabilities. Its primary function is to promote transparency and greater responsibility in the transfer of conventional arms and dual-use goods and technologies. By adhering to a set of agreed guidelines, the participating countries work to ensure that their exports do not contribute to regional or global instability. This arrangement focuses on both preventing the proliferation of weapons and fostering cooperation among nations about responsible arms transfers. It is particularly significant in a context where technological advancements may lead to an arms race or increased tensions between nations. The Wassenaar Arrangement thus plays a crucial role in maintaining international security and stability. The other options, such as e-Discovery and encryption laws, relate to specific legal and technological frameworks rather than arms control or international security measures. Export laws generally encompass a broader range of regulations that may affect the transfer of goods, but they do not specifically target the prevention of military destabilization in the same focused manner as the Wassenaar Arrangement does.

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://wgu-itas6291d488.examzify.com

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

SAMPLE