Western Governors University (WGU) ITAS6291 D488 Cybersecurity Architecture and Engineering Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit:
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. **Which standard addresses IT security techniques, including the introduction and general model, as well as functional and assurance components?**
    - **A. NIST 800-61 (Computer Security Incident Handling Guide)**
    - **B. ISO standard 15408**
    - **C. NIST 800-84**
    - **D. NIST 800-53 (Security and Privacy Controls for Information Systems)**

2. **While patching may help prevent catastrophic events, why is it not considered part of the Business Impact Analysis (BIA)?**
    - **A. Because it is the first step in business continuity planning**
    - **B. Because it is focused on inventory management**
    - **C. Because it addresses system vulnerabilities, not the impact analysis**
    - **D. Because it is the final step in the BIA process**

3. **What approach is used in key management to ensure proper identification and ownership of keys?**
    - **A. Dispersion**
    - **B. Bound (Ownership binding)**
    - **C. Rotation**
    - **D. Storage consideration**

4. **What data sanitization method involves destroying the decryption key to make data recovery impossible?**
    - **A. Format (Quick Format)**
    - **B. Disk Defragmentation**
    - **C. Purge**
    - **D. Crypto erase**

SAMPLE

5. **Which actions can ensure the integrity and authenticity of a company's cloud infrastructure?**

   A. **Implementing attestation services**

   B. **Implementing a load balancer to distribute traffic**

   C. **Conducting regular vulnerability assessments and penetration testing**

   D. **Using a web application firewall**

6. **Which test ensures that a particular block of code performs the exact action intended and provides the exact output expected?**

   A. **A. Regression test**

   B. **B. Integration test**

   C. **C. Unit test**

   D. **D. Solution design**

7. **Which EAP (Extensible Authentication Protocol) type is similar to PEAP (Protected Extensible Authentication Protocol) but uses a Protected Access Credential (PAC) instead of a certificate to set up the tunnel?**

   A. **EAP-TTLS (EAP Tunneled TLS)**

   B. **EAP-FAST (EAP with Flexible Authentication via Secure Tunneling)**

   C. **EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)**

   D. **PEAP (Protected Extensible Authentication Protocol)**

8. **A network administrator is searching for an open source network access control (NAC) solution to integrate with the company's public key infrastructure (PKI) environment. Which of the following could the administrator use?**

   A. **PacketFence**

   B. **Secure Authentication**

   C. **Software Guard Extension**

   D. **Poly1305**

SAMPLE

9. **In a data loss prevention system, what action involves preventing all access to original files while notifying the user?**

   A. **A. Block**

   B. **B. Alert**

   C. **C. Quarantine**

   D. **D. Tombstone**

10. **Which type of threat actor arises from an individual whom the organization has identified and granted access?**

    A. **Hacktivist**

    B. **Organized crime**

    C. **Insider threat**

    D. **Competitor**

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. **Which standard addresses IT security techniques, including the introduction and general model, as well as functional and assurance components?**

   A. NIST 800-61 (Computer Security Incident Handling Guide)

   B. ISO standard 15408

   C. NIST 800-84

   D. NIST 800-53 (Security and Privacy Controls for Information Systems)

The correct choice relates to ISO standard 15408, also known as the Common Criteria for Information Technology Security Evaluation. This standard provides a comprehensive framework for evaluating the security features and capabilities of IT products and systems. It introduces a general model of IT security and delineates functional components, specifying what a product or system needs to have in order to meet certain security standards. ISO 15408 focuses on defining security assurance requirements and evaluating the security functionality of various IT products. This standard serves as a benchmark for product security evaluations, enabling organizations to assess whether products meet specific security requirements. Its structured approach assists in the design, development, and evaluation stages of IT systems, ensuring that they are robust against potential security threats. The other options discuss different aspects of IT security but do not encompass the same breadth. For instance, NIST 800-61 is focused on incident handling procedures rather than a holistic evaluation framework. NIST 800-84 deals with the creation of contingency plans, while NIST 800-53 specifies security and privacy controls for federal information systems but does not provide an overarching model or standard for the evaluation process. Each of these has its specific focus, making ISO 15408 the most suitable choice for addressing comprehensive IT security techniques.

2. **While patching may help prevent catastrophic events, why is it not considered part of the Business Impact Analysis (BIA)?**

   A. Because it is the first step in business continuity planning

   B. Because it is focused on inventory management

   C. Because it addresses system vulnerabilities, not the impact analysis

   D. Because it is the final step in the BIA process

SAMPLE

Patching is typically focused on addressing specific vulnerabilities in systems, which is a critical aspect of maintaining security. However, the Business Impact Analysis (BIA) aims to assess the potential impact of disruptions on business operations. While patching may help reduce the likelihood of incidents that could lead to disruptions, it does not itself evaluate how those disruptions would affect the organization. The essence of a BIA is to analyze the significance of various business functions and the consequences of their downtime. This involves identifying critical processes, estimating the impact of loss on those processes, and determining recovery priorities. Patching is a tactical measure to mitigate risks but does not consider the broader business implications of downtime, which is what the BIA focuses on. Thus, while patching supports overall security posture, it is not within the scope of the BIA since it does not assess the impacts on business performance and continuity.

3. What approach is used in key management to ensure proper identification and ownership of keys?

A. Dispersion

B. Bound (Ownership binding)

C. Rotation

D. Storage consideration

The approach used in key management to ensure proper identification and ownership of keys is known as ownership binding. This practice helps to establish a clear association between the keys and the entities that own or are responsible for them. By binding keys to specific individuals or systems, it becomes easier to manage access controls, hold users accountable for key usage, and maintain a robust security posture. Ownership binding typically involves mechanisms to verify the identity of key holders and may integrate with identity management solutions. This ensures that only authorized personnel can access or use the keys, reducing the risk of unauthorized access to sensitive data or systems. This concept is a critical part of maintaining integrity and trust in cryptographic operations and overall security architecture. In contrast, dispersion refers to the distribution of keys across multiple locations to prevent single points of failure, while rotation focuses on the regular updating and changing of keys to enhance security. Storage consideration relates to how keys are stored securely to prevent unauthorized access, but it does not directly address the issue of ownership and accountability like ownership binding does.

4. What data sanitization method involves destroying the decryption key to make data recovery impossible?

A. Format (Quick Format)

B. Disk Defragmentation

C. Purge

D. Crypto erase

The data sanitization method that involves destroying the decryption key to make data recovery impossible is referred to as "crypto erase." This method is particularly effective because, when the decryption key is destroyed, the data that was encrypted with it becomes irretrievable. Essentially, the data itself may still exist on the storage medium, but it is rendered useless, as there is no way to decrypt it without the key. Crypto erase is an essential technique in data protection, especially when decommissioning storage devices or ensuring compliance with data privacy regulations. By utilizing this method, organizations can ensure that sensitive information cannot be accessed or recovered, thereby significantly minimizing the risk of data breaches or unauthorized access to confidential information. This contrasts with other methods of data sanitization, which may not provide the same level of certainty in preventing data recovery.

SAMPLE

5. Which actions can ensure the integrity and authenticity of a company's cloud infrastructure?

A. Implementing attestation services

B. Implementing a load balancer to distribute traffic

C. Conducting regular vulnerability assessments and penetration testing

D. Using a web application firewall

Implementing attestation services is a crucial action for ensuring the integrity and authenticity of a company's cloud infrastructure. Attestation services work by allowing systems to verify that the software and configurations running on a machine are in a known, trusted state. This process involves cryptographic techniques to establish trust through remote validation of the hardware and software states. Attestation helps to confirm that a system has not been tampered with and that it remains compliant with security policies, which is vital in a cloud environment where multiple tenants may share resources. By providing assurance that the infrastructure is operating as intended, attestation services reinforce the integrity of data and applications hosted in the cloud, thus protecting against various cyber threats and breaches. Other security measures, while valuable in their own right, do not directly address the verification of system integrity and authenticity as effectively as attestation services do. For instance, a load balancer distributes traffic to ensure performance and availability, but it does not provide verification of the underlying systems. Similarly, regular vulnerability assessments help identify weaknesses, and web application firewalls protect applications from specific types of threats, but they do not confirm the integrity of the cloud infrastructure itself.

6. Which test ensures that a particular block of code performs the exact action intended and provides the exact output expected?

A. A. Regression test

B. B. Integration test

C. C. Unit test

D. D. Solution design

A unit test is specifically designed to validate that a particular block of code, typically a function or method, performs its intended action and produces the expected output. It focuses on a small segment of the code to ensure that it behaves as intended under specified conditions. Unit tests are usually written by developers as they write the code, enabling them to check that each individual component functions correctly before integrating it into larger systems. This approach is crucial in identifying bugs at an early stage in the development process, as it isolates each part of the program and tests it independently. The primary goal of a unit test is to make sure that the code meets its requirements on a granular level, ensuring reliability and maintainability throughout the software development lifecycle. Other testing methods serve different purposes. For instance, regression tests check that new code changes haven’t adversely affected existing functionality, while integration tests confirm that different modules or services work together correctly. Solution design, on the other hand, is a part of the planning process in development and does not involve testing code execution or output.

SAMPLE

7. Which EAP (Extensible Authentication Protocol) type is similar to PEAP (Protected Extensible Authentication Protocol) but uses a Protected Access Credential (PAC) instead of a certificate to set up the tunnel?

A. EAP-TTLS (EAP Tunneled TLS)

B. EAP-FAST (EAP with Flexible Authentication via Secure Tunneling)

C. EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)

D. PEAP (Protected Extensible Authentication Protocol)

The correct choice is EAP-FAST (EAP with Flexible Authentication via Secure Tunneling) because it establishes an authenticated tunnel using a Protected Access Credential (PAC) rather than relying on a digital certificate. This mechanism allows for a lightweight and flexible approach to secure authentication, making it suitable for environments where certificate management may be cumbersome or not feasible. EAP-FAST creates a secure tunnel to protect subsequent authentication exchanges, and using a PAC simplifies the setup compared to protocols that require full public key infrastructure (PKI) for certificate management. This makes EAP-FAST attractive for organizations looking to address scalability and deployment ease while maintaining a high level of security. Other similar protocols, such as EAP-TTLS and PEAP, use certificates for the establishment of their secure tunnels. EAP-TTLS, while also creating a secure tunnel, relies on a server-side certificate, and PEAP similarly requires server-side certificates and offers user authentication inside a secure tunnel. EAP-TLS, on the other hand, is based on mutual authentication using certificates for both the client and server, which involves more complexity concerning certificate management.

8. A network administrator is searching for an open source network access control (NAC) solution to integrate with the company's public key infrastructure (PKI) environment. Which of the following could the administrator use?

A. PacketFence

B. Secure Authentication

C. Software Guard Extension

D. Poly1305

PacketFence is recognized as a robust open-source network access control (NAC) solution that can effectively integrate with various environments, including those utilizing a public key infrastructure (PKI). It offers features that facilitate network visibility, control, and compliance, making it suitable for organizations looking to establish secure access policies based on user identity and device security status. The integration with PKI is particularly significant because PacketFence can leverage PKI for authentication mechanisms, ensuring that devices authenticated through certificates can join the network without compromising security. This aligns well with the goals of NAC, which are to enforce security policy compliance and manage access to the network based on device and user identity. The other choices do not serve the role of an open-source NAC solution specifically tailored for integration with PKI. Secure Authentication is a broader term that does not refer to a specific NAC product, while Software Guard Extensions (SGX) are focused on providing a trusted execution environment rather than network access control. Poly1305 is a cryptographic message authentication code and does not pertain to NAC solutions. Thus, PacketFence stands out as the most appropriate option for the given scenario.

SAMPLE

9. In a data loss prevention system, what action involves preventing all access to original files while notifying the user?

A. A. Block

B. B. Alert

C. C. Quarantine

D. D. Tombstone

In a data loss prevention (DLP) system, the action that involves preventing all access to original files while notifying the user is known as "quarantine." When files are quarantined, they are isolated from users, effectively blocking access to them to prevent any potential data breaches or leaks. This is crucial in maintaining data integrity and security, as it acts as a preventative measure until the file can be reviewed, assessed, and deemed safe for access again. The process of quarantining not only restricts access but also typically generates a notification for the user, informing them that their access to certain files has been limited due to a potential risk identified by the DLP system. This dual action of blocking access and providing notification helps ensure users are aware of security measures being enforced without compromising the data. In contrast, the other options reflect different actions involving data management and user notifications. "Block" refers merely to stopping access without the notification aspect, "alert" pertains to informing the user about a potential issue without restricting access, and "tombstone" generally refers to marking an entry as inactive without directly managing access to files.

10. Which type of threat actor arises from an individual whom the organization has identified and granted access?

A. Hacktivist

B. Organized crime

C. Insider threat

D. Competitor

The correct answer is the insider threat. This type of threat actor arises from individuals within the organization who have been granted access to its systems and data. Unlike external threats, insider threats can be more challenging to detect and mitigate because these individuals are already trusted users with legitimate credentials. They may have knowledge about the organization's internal processes, resources, and security measures, which can make their malicious actions even more damaging. Insider threats can manifest in various ways, such as data theft, sabotage, or the misuse of access privileges for personal gain. Because they originate from within the organization, detecting and preventing insider threats often requires a combination of monitoring user behavior, implementing access controls, and fostering a culture of security awareness among employees. While other options like hacktivists, organized crime, and competitors represent external threats, they do not stem from individuals who have been granted internal access to the organization's resources. This distinction is essential for understanding the unique challenges posed by insider threats within cybersecurity frameworks.

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