INFORMATION SYSTEMS SECURITY ARCHITECTURE PROFESSIONAL (ISSAP) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://issap.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 term guards against improper information modification or destruction and includes ensuring information non-repudiation and authenticity?**

   A. Integrity

   B. Least Privilege

   C. Forensics

   D. Firewalls

2. **What is the purpose of a Business Impact Analysis?**

   A. A formal assessment of financial impact in the event of a disaster.

   B. A plan for migrating to cloud services.

   C. A list of assets with criticality reflecting their importance to the organization.

   D. A schedule for employee training on security policies.

3. **Dynamic Testing is testing of the functionality of software; also known as black box testing.**

   A. Dynamic Testing

   B. Entitlement

   C. Privileged Accounts

   D. Proof of Possession

4. **Which statement accurately defines Layered Defense when protecting assets?**

   A. The use of a single, strong control to protect an asset.

   B. The use of multiple controls arranged in series to provide multiple consecutive protections.

   C. An approach that relies solely on encryption to protect data.

   D. An approach that eliminates all controls for efficiency.

5. **What is data classification, and how does it influence security controls?**

   A. Data classification assigns sensitivity levels (confidential, internal, public); controls are selected and enforced based on classification to protect data appropriately.

   B. Data classification sets encryption keys automatically.

   C. Data classification determines the physical storage location only.

   D. Data classification has no impact on security controls.

SAMPLE

6. Privileged Accounts are accounts on a system with higher levels of permissions.

A. Proof of Possession

B. Dynamic Testing

C. Privileged Accounts

D. Virtual Machines

7. Which activity is described as the attempt to enter a system or network through an unauthorized channel?

A. Policy

B. Risk Management

C. Legacy IT Systems

D. Penetration Testing

8. What describes the role of physical security within ISSAP and its integration with cyber security?

A. Physical security protects hardware, facilities, personnel; integrated with cyber security to prevent tampering, theft, and environmental threats, often via layering and surveillance.

B. Physical security is entirely separate from cyber security.

C. Physical security only concerns badge access.

D. Physical security is irrelevant to ISSAP.

9. Which statement best describes data encryption at rest?

A. Data at rest encryption protects stored data using algorithms like AES, or disk encryption

B. It only protects data in transit

C. It uses only DES

D. It is unnecessary if network is private

10. In many enterprise architecture frameworks, security is treated as what?

A. Security is rarely considered in architecture.

B. Security is treated as a cross-cutting concern that affects multiple domains.

C. Security is only applied to data centers.

D. Security is irrelevant to business goals.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which term guards against improper information modification or destruction and includes ensuring information non-repudiation and authenticity?

A. Integrity

B. Least Privilege

C. Forensics

D. Firewalls

Integrity is the concept that guards against improper information modification or destruction by ensuring data remains accurate and complete and that any changes can be detected or prevented. It also ties in with non-repudiation and authenticity: digital signatures, hash values, and audit trails provide proof of origin and integrity, so a sender cannot deny sending data and a recipient can verify the data truly comes from a legitimate source and has not been altered. The other options address different goals—least privilege limits who can do what, forensics deals with investigating after an incident, and firewalls control network traffic—none of which directly ensure data remains unmodified, while also guaranteeing non-repudiation and authenticity.

2. What is the purpose of a Business Impact Analysis?

A. A formal assessment of financial impact in the event of a disaster.

B. A plan for migrating to cloud services.

C. A list of assets with criticality reflecting their importance to the organization.

D. A schedule for employee training on security policies.

The purpose of a Business Impact Analysis is to identify which assets and processes are essential to the organization and to rank them by how critical they are to operations. It involves mapping business activities to the systems, data, facilities, and people they depend on, and assessing the potential consequences of disruptions for each asset or process. This establishes recovery priorities and tolerances, such as how quickly things must be restored (RTO) and how much data loss is acceptable (RPO), guiding where to focus resilience and recovery efforts. This focus on prioritizing assets by importance makes it the best fit, rather than plans for cloud migration or training schedules, or a narrow financial impact assessment.

3. Dynamic Testing is testing of the functionality of software; also known as black box testing.

A. Dynamic Testing

B. Entitlement

C. Privileged Accounts

D. Proof of Possession

Dynamic testing evaluates what the software does while it runs. By executing the program with real inputs, you observe outputs, behavior, and state changes to verify it meets its requirements. Because you focus on external behavior rather than how the code is written or structured inside, this approach aligns with black box testing. Functional testing, regression testing, and user-acceptance style checks are classic examples of this dynamic, runtime-focused approach. The other terms are not testing approaches: entitlement refers to the permissions assigned to a user, privileged accounts are high-access human or service accounts, and proof of possession is a cryptographic concept used to verify you hold a credential or key. They relate to access control and cryptography, not to how testing is performed.

SAMPLE

4. Which statement accurately defines Layered Defense when protecting assets?

A. The use of a single, strong control to protect an asset.

B. The use of multiple controls arranged in series to provide multiple consecutive protections.

C. An approach that relies solely on encryption to protect data.

D. An approach that eliminates all controls for efficiency.

Layered defense means building multiple protections across different stages so an attacker must overcome several barriers to reach an asset. The strongest fit describes several controls arranged in series to create successive barriers. With this setup, even if one control is bypassed or fails, others still stand in the way, reducing risk and slowing or stopping an attack as it moves through network, host, application, and data layers. This redundancy covers different attack paths and creates defense in depth, rather than relying on a single control. Encryption alone targets confidentiality but doesn't provide the full multi-layered protection; removing controls eliminates the protective barriers, increasing exposure.

5. What is data classification, and how does it influence security controls?

A. Data classification assigns sensitivity levels (confidential, internal, public); controls are selected and enforced based on classification to protect data appropriately.

B. Data classification sets encryption keys automatically.

C. Data classification determines the physical storage location only.

D. Data classification has no impact on security controls.

Data classification assigns levels of sensitivity and criticality to data, and it directly guides what protections should be in place. When data is labeled as confidential, internal, or public, organizations can tailor controls to match the risk, applying stronger measures where needed and lighter ones where appropriate. This means choosing and enforcing access controls (who can view or modify the data), authentication and authorization requirements, encryption (at rest and in transit) and key management policies, monitoring and auditing, data handling procedures, and how data is stored, shared, retained, and destroyed. The idea is to align protection with risk: highly sensitive or regulated data receives strict protections, while public data requires fewer controls. This classification also supports compliance and lifecycle management, ensuring that as data moves through creation, storage, use, sharing, and disposal, the security controls follow it accordingly. Claims that classification only sets encryption keys or only determines where data is stored are too narrow. Encryption choices are informed by classification but not automatically assigned as keys; storage location decisions are just one aspect, not the whole picture. And saying it has no impact ignores how classification drives the selection and enforcement of all relevant security controls.

SAMPLE

6. Privileged Accounts are accounts on a system with higher levels of permissions.

A. Proof of Possession

B. Dynamic Testing

C. Privileged Accounts

D. Virtual Machines

Privileged accounts are those with elevated permissions that allow administrators to configure systems, install software, manage other users, and access sensitive settings. This distinction is essential for effective access control, enforcing the least privilege principle, and enabling proper auditing and monitoring of sensitive actions. The statement directly describes what privileged accounts are, so naming this concept is the most accurate fit. The other options don't describe account types or permissions: proof of possession relates to proving you possess a credential, not to the level of access; dynamic testing is a testing approach used to find vulnerabilities during operation; virtual machines are computing environments, not a description of user accounts or permissions.

7. Which activity is described as the attempt to enter a system or network through an unauthorized channel?

A. Policy

B. Risk Management

C. Legacy IT Systems

D. Penetration Testing

Penetration testing is about simulating an attacker by attempting to breach a system or network through channels an attacker might use, all within a controlled and authorized scope. This practice aims to uncover vulnerabilities, test defenses, and measure how well access controls, network segmentation, and monitoring stand up to real intrusion techniques. The activity is designed to reveal what could be exploited and how detections and responses would perform, so remediation can be planned accordingly. In contrast, policy governs rules and behavior, risk management covers identifying and mitigating risks, and legacy IT systems refer to old technology—not the act of attempting unauthorized entry.

SAMPLE

8. What describes the role of physical security within ISSAP and its integration with cyber security?

A. Physical security protects hardware, facilities, personnel; integrated with cyber security to prevent tampering, theft, and environmental threats, often via layering and surveillance.

B. Physical security is entirely separate from cyber security.

C. Physical security only concerns badge access.

D. Physical security is irrelevant to ISSAP.

Physical security in ISSAP is about protecting the tangible assets that enable information systems—hardware, facilities, and the people who interact with them—and doing so in a way that integrates with cyber security to create a layered, coordinated defense. This integration ensures that threats like tampering, theft, and environmental risks are addressed across both physical and digital domains, strengthening overall resilience. The approach involves multiple controls working together: securing facilities and rooms, tamper-evident seals and secure enclosures for hardware, access control and authentication for personnel, surveillance such as cameras, and environmental protections like fire suppression and climate control. It also includes supply-chain safeguards and coordinated incident response with cyber monitoring so that a breach in one domain doesn't automatically cascade into the other. This holistic view is why the option describing a combined, layered effort that protects hardware, facilities, and people—and prevents tampering, theft, and environmental threats through surveillance and integrated controls—is the best fit. Physical security being separate from cyber security isn't accurate because ISSAP treats security as an integrated system. Limiting physical security to badge access is too narrow to capture the breadth of protections required. Saying physical security is irrelevant to ISSAP contradicts the core goal of safeguarding all elements that support information systems.

9. Which statement best describes data encryption at rest?

A. Data at rest encryption protects stored data using algorithms like AES, or disk encryption

B. It only protects data in transit

C. It uses only DES

D. It is unnecessary if network is private

Data encryption at rest protects stored information by making it unreadable without the proper key. It secures data when it sits on disks, databases, backups, or portable media, so even if someone gains access to the storage, they can't read the data without decryption keys. This is usually done with strong algorithms such as AES and methods like full-disk or database-level encryption. It's important to distinguish this from data in transit, which is protected while moving over networks (for example, with TLS or IPsec). DES is an older algorithm and not representative of current best practice; modern implementations rely on AES or stronger. The idea that encryption at rest isn't needed if the network is private isn't correct, because threats can arise from physical access to storage or compromised backups regardless of network exposure.

SAMPLE

10. In many enterprise architecture frameworks, security is treated as what?

A. Security is rarely considered in architecture.

B. Security is treated as a cross-cutting concern that affects multiple domains.

C. Security is only applied to data centers.

D. Security is irrelevant to business goals.

Security is treated as a cross-cutting concern that affects multiple domains across enterprise architecture. Because architecture covers business processes, data, applications, and technology infrastructure, security needs to be woven into every layer and view from the start. This means security requirements, controls, risk management, and governance aren't added late in the project but are embedded in strategy, data handling, system design, and deployment decisions. Such integration helps ensure consistent protection, regulatory compliance, and resilience across the entire enterprise, and it aligns security with business objectives rather than treating it as a separate or after-the-fact concern. Saying security is rarely considered is inconsistent with how modern frameworks operate, which emphasize pervasive security consideration. Limiting security to data centers misses the broader scope of cloud, networks, endpoints, identities, and data flows. Declaring security irrelevant to business goals ignores the direct impact security has on trust, continuity, and regulatory compliance.

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://issap.examzify.com

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

SAMPLE