DSAC ANNEX F PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://dsacannexf.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 15

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 incident containment and which strategies help achieve it?

A. Eliminating all risk from the system.

B. Limiting spread; network segmentation, isolating affected assets, and removing attacker footholds.

C. Waiting for the attacker to leave before acting.

D. Only logging events without taking action.

2. Which access control model assigns permissions primarily by the owner?

A. Discretionary Access Control (DAC) assigns permissions primarily by the resource owner.

B. Mandatory Access Control (MAC) assigns permissions based on fixed levels.

C. Role-Based Access Control (RBAC) assigns permissions by user roles.

D. Attribute-Based Access Control (ABAC) uses attributes.

3. How should cryptographic algorithms be chosen and updated under Annex F?

A. Based on vendor popularity

B. Based on current standards, strength tests, import/export considerations, and update path for deprecation

C. Randomly selected for each project

D. Based solely on fastest computation time

4. In multi-agent networks, what is a SuperAgent?

A. Agents designated to act as a source of content updates to other agents in the same network

B. A primary user account with admin rights

C. A firewall module managing traffic

D. A data backup daemon

5. Which of the following is NOT a type of malware?

A. Viruses

B. Worms

C. Trojan horses

D. Firewall

SAMPLE

6. What is the core principle of zero trust in DSAC Annex F?

A. Rely On Perimeter Defenses

B. Verify At Every Access Attempt

C. Trust No One By Default

D. Assume Internal Networks Are Trusted

7. HBSS is designed to provide local security against cyber threats. Which option best represents this function?

A. Threats

B. Viruses only

C. Network intrusions only

D. Data loss

8. Social Engineering is defined as:

A. An attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected.

B. An attack that breaks encryption

C. A method of securing passwords

D. A technique to optimize networks

9. Which statement correctly describes encryption in transit and at rest?

A. In transit protects stored data; at rest protects data moving across networks.

B. In transit protects data moving across networks; at rest protects stored data. Use both as required by data sensitivity and regulatory requirements.

C. In transit and at rest both protect data only during processing.

D. In transit protects data at rest and in transit not needed.

10. Which item is NOT one of the three primary information security principles?

A. Accountability

B. Confidentiality

C. Integrity

D. Availability

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is incident containment and which strategies help achieve it?

A. Eliminating all risk from the system.

B. Limiting spread; network segmentation, isolating affected assets, and removing attacker footholds.

C. Waiting for the attacker to leave before acting.

D. Only logging events without taking action.

Containment focuses on stopping the attacker from spreading and limiting the damage after a breach is detected. The best approach uses concrete actions that immediately curb the attacker's reach: network segmentation to restrict movement between parts of the environment, isolating affected assets so compromised systems can't communicate with others, and removing attacker footholds by eradicating backdoors, compromised credentials, and malware. These steps reduce the blast radius and create a safer window to perform thorough eradication and recovery. Others are not suitable because eliminating all risk right away isn't realistic during an active incident, waiting for the attacker to leave is passive and allows further harm, and simply logging events without taking action fails to stop ongoing activity and containment.

2. Which access control model assigns permissions primarily by the owner?

A. Discretionary Access Control (DAC) assigns permissions primarily by the resource owner.

B. Mandatory Access Control (MAC) assigns permissions based on fixed levels.

C. Role-Based Access Control (RBAC) assigns permissions by user roles.

D. Attribute-Based Access Control (ABAC) uses attributes.

Discretionary Access Control centers on the resource owner having the authority to grant or revoke access. The owner attaches an access control list or similar policy to the resource, and can decide which users or groups are allowed to read, write, or execute. This makes permissions primarily driven by the owner's discretion, giving flexibility to share with specific individuals while keeping others out. This contrasts with other models: Mandatory Access Control uses fixed, centralized rules based on security labels rather than owner decisions; Role-Based Access Control assigns permissions by user roles rather than by who owns the resource; Attribute-Based Access Control uses attributes of the user, resource, and environment to determine access. A typical file system example illustrates the idea: the file owner can set who else can access that file and what they can do with it, whereas in the other models those kinds of owner-driven decisions aren't the primary mechanism.

SAMPLE

3. How should cryptographic algorithms be chosen and updated under Annex F?

A. Based on vendor popularity

B. Based on current standards, strength tests, import/export considerations, and update path for deprecation

C. Randomly selected for each project

D. Based solely on fastest computation time

Selecting cryptographic algorithms and planning their updates under Annex F should follow standards, be backed by strength testing, consider import/export constraints, and include a clear deprecation/update path. Relying on current standards ensures interoperability and a recognized security baseline that many organizations rely on. Strength tests confirm that an algorithm actually resists known attacks in practice, not just in theory, giving real assurance about its resilience. Import/export considerations address legal and regulatory constraints that can affect which algorithms you may use in different regions or for different partners. Finally, an explicit update path for deprecation ensures you can migrate to stronger algorithms before weaknesses are exploited, maintaining confidentiality and integrity over time. Choosing based on popularity or speed alone ignores security guarantees and lifecycle risk, and random selection would introduce instability and potential vulnerabilities.

4. In multi-agent networks, what is a SuperAgent?

A. Agents designated to act as a source of content updates to other agents in the same network

B. A primary user account with admin rights

C. A firewall module managing traffic

D. A data backup daemon

In multi-agent networks, content distribution and synchronization are key ideas. A SuperAgent is an agent designated to serve as the source of content updates for the rest of the network. It hosts or creates the updated content and coordinates its delivery to the other agents, helping everyone stay on the same page as information changes. This hub role simplifies propagation, reduces conflicting updates, and ensures peers receive the latest content from a central update source. It's about moving and coordinating information, not about administrative control, security filtering, or data backups. For example, when the central feed is refreshed, the SuperAgent pushes the new content to all connected agents so their local states reflect the newest information.

5. Which of the following is NOT a type of malware?

A. Viruses

B. Worms

C. Trojan horses

D. Firewall

Malware is software designed to harm, steal, or gain unauthorized access, and the items that fit that description include viruses, worms, and Trojan horses. A virus attaches itself to a host program and spreads when that program runs; a worm copies itself across networks without user action; a Trojan horse disguises itself as something legitimate to trick you into executing it. A firewall, by contrast, is a defensive tool that monitors and controls incoming and outgoing network traffic to block unauthorized access. It doesn't spread, replicate, or cause damage itself; its purpose is to prevent harm. So the firewall is not malware.

SAMPLE

6. What is the core principle of zero trust in DSAC Annex F?

A. Rely On Perimeter Defenses

B. Verify At Every Access Attempt

C. Trust No One By Default

D. Assume Internal Networks Are Trusted

Zero trust begins with the idea that nothing should be trusted by default, inside or outside the network. Access is granted only after thorough verification of identity, device health, and context, and this verification happens for every access attempt. That makes "trust no one by default" the best way to express the overall principle, because it captures the default posture that drives the entire approach: you don't assume anyone or any device is trustworthy simply for being on the network. Verification and authorization are continuous and context-driven, rather than relying on a fixed perimeter or assuming internal entities are safe. The other options imply relying on a boundary or trusting internal networks, which runs opposite to zero trust.

7. HBSS is designed to provide local security against cyber threats. Which option best represents this function?

A. Threats

B. Viruses only

C. Network intrusions only

D. Data loss

HBSS operates at the endpoint to provide local protection against cyber threats. The best fit is threats because HBSS is designed to defend a host against a wide range of harmful activities—from malware and intrusions to data leakage and other attacks—on the device itself. Limiting the option to viruses only or network intrusions only misses this broad protective role, and treating data loss as the threat focuses on a consequence rather than the wide variety of threat types HBSS aims to prevent.

8. Social Engineering is defined as:

A. An attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected.

B. An attack that breaks encryption

C. A method of securing passwords

D. A technique to optimize networks

Social engineering targets people by exploiting psychology to bypass security controls. It relies on human interaction to trick someone into breaking a security procedure or revealing sensitive information that should be protected, rather than breaking technical defenses directly. This is why the described option is the best fit: it captures the essence of manipulating a person to gain access or data. In contrast, other ideas refer to technical breaches of encryption, or to methods for protecting passwords, or to network optimization—topics that don't involve tricking people to circumvent safeguards. Examples include phishing, pretexting, or tailgating, where the attacker uses trust, urgency, or fear to prompt the user into action. Mitigation centers on training, awareness, and strong controls like multi-factor authentication to reduce the risk.

SAMPLE

9. Which statement correctly describes encryption in transit and at rest?

A. In transit protects stored data; at rest protects data moving across networks.

B. In transit protects data moving across networks; at rest protects stored data. Use both as required by data sensitivity and regulatory requirements.

C. In transit and at rest both protect data only during processing.

D. In transit protects data at rest and in transit not needed.

Encryption serves two distinct moments in the data lifecycle: when data is moving and when it is stored. Encryption in transit protects data as it travels across networks, using protocols like TLS to prevent anyone who intercepts the traffic from reading it. Encryption at rest protects data that is stored on disks, databases, or backup media, ensuring that someone who gains physical access to the storage cannot read the data without the proper keys. Because data often moves between systems and then sits in storage, you typically implement both protections, choosing the level of protection based on how sensitive the data is and any regulatory requirements. For example, you'd encrypt data in transit (to protect it during transmission) and encrypt stored data (to protect it when at rest) and manage keys securely to enforce access controls.

10. Which item is NOT one of the three primary information security principles?

A. Accountability

B. Confidentiality

C. Integrity

D. Availability

The main idea here is the CIA triad, which covers three core security goals: confidentiality, integrity, and availability. Confidentiality means only authorized people can access information; integrity ensures data is accurate and not tampered with; availability guarantees that authorized users can access the data and systems when needed. Accountability plays an important role in security by ensuring actions can be traced and responsibilities assigned (think logs, audits, and non-repudiation), but it is not one of the three primary goals of the CIA triad. That's why the item describing accountability is not part of the three primary information security principles. The other terms—confidentiality, integrity, and availability—are the triad.

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://dsacannexf.examzify.com

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

SAMPLE