DSAC ANNEX F PRACTICE TEST (SAMPLE)

STUDY GUIDE

Prepare with structure. Pass with confidence

Table of Contents

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.

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!

Questions

1. Operations Security is best described as which of the following?

A. Protection and risk management process that classifies information, then determines what is required to protect sensitive information and prevent it from getting into the wrong hands

B. A purely technical firewall configuration

C. User password management only

D. Dataset anonymization procedures

2. Which statement best describes the principle of least privilege?

A. Granting users the maximum rights needed.

B. Providing users only the minimum rights necessary.

C. Regularly auditing all privileges.

D. Disabling all user permissions.

3. A Certificate Authority is:

A. An entity that issues and signs digital certificates with identity and a key

B. A hardware device used to store certificates

C. A firewall feature

D. A software for password management

4. DDoS attacks are Attacks that utilize multiple systems to disrupt the traffic of a targeted systems by flooding the target with too much information in order to slow or crash the intended target(s).

A. Attacks that utilize multiple systems to disrupt the traffic of a targeted systems by flooding the target with too much information in order to slow or crash the intended target(s).

B. A method of data exfiltration

C. A technique to secure networks

D. A form of malware

5. PKI is described as a framework.

A. True

B. False

C. It depends

D. Not sure

6. CTO is an acronym in DoD cyber policy. What does CTO stand for?

A. Cyber Tasking Order
B. Cyber Technical Operation
C. Cyber Tasking Oversight
D. Critical Task Order

7. Which unit is responsible for executing DODIN and DCO operations?

A. Marine Corps Cyberspace Operations Group (MCCOG)
B. DISA
C. NSA
D. USCYBERCOM

8. Critical Infrastructure security refers to which of the following?

A. The physical and cyber systems that are vital to the United States
B. Only government networks
C. Individual personal devices
D. Cloud service configurations

9. Which of the following is a countermeasure related to access control?

A. Biometric authentication systems
B. Phishing emails
C. Unencrypted data transfer
D. Public Wi-Fi access

10. Which mechanism records user actions for auditing?

A. Authentication
B. Auditing
C. Accounting
D. Authorization

Answers

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

Explanations

1. Operations Security is best described as which of the following?

A. Protection and risk management process that classifies information, then determines what is required to protect sensitive information and prevent it from getting into the wrong hands

B. A purely technical firewall configuration

C. User password management only

D. Dataset anonymization procedures

Operations Security centers on protecting information by applying a risk-based approach that covers people, processes, and technology. It starts with identifying what information is sensitive through classification, then determining the protections required to safeguard that information and prevent disclosure or loss. This broad view goes beyond any single control, aiming to manage risk across the entire lifecycle of information. That's why the best description is a protection-and-risk-management process that classifies information and then decides what's needed to guard it and keep it from the wrong hands. A purely technical firewall configuration only addresses network barriers and misses the broader risk-based protection of all sensitive data. Focusing only on user passwords ignores other sensitive information and the procedural and organizational controls involved. Dataset anonymization concentrates on privacy of data rather than the full security posture and handling of sensitive information across an organization.

2. Which statement best describes the principle of least privilege?

A. Granting users the maximum rights needed.

B. Providing users only the minimum rights necessary.

C. Regularly auditing all privileges.

D. Disabling all user permissions.

Providing users only the minimum rights necessary to perform their tasks is the essence of the least privilege principle. This approach limits what an account can do, so even if credentials are compromised or a user makes a mistake, the potential damage stays small. It also makes security management clearer: with the smallest possible set of permissions, it's easier to enforce controls, track actions, and apply the right level of access for each role. In practice, a user who only needs to view reports wouldn't have the ability to change configurations, and elevated rights would be granted only temporarily for a specific task. Granting maximum rights would dramatically increase risk, since users would have broad access beyond what they need. Regularly auditing privileges is important for governance and maintaining appropriate access over time, but it describes ongoing oversight rather than the core idea of giving the minimum necessary access. Disabling all permissions would render work impossible.

3. A Certificate Authority is:

A. An entity that issues and signs digital certificates with identity and a key

B. A hardware device used to store certificates

C. A firewall feature

D. A software for password management

In PKI, a Certificate Authority is the trusted entity that issues digital certificates and signs them to bind an identity to a public key. It verifies who the certificate holder claims to be, issues a certificate that contains the holder's identity information and public key, and then signs that certificate with its private key. Anyone receiving the certificate can verify that signature using the CA's public key, which is trusted because it's provided by a root CA already installed in the relying party's trust store. This creates a chain of trust: if the certificate is valid and signed by a trusted CA, the identity and key are trusted for secure communication. This role is distinct from storing certificates in a hardware device (like a secure storage module), from firewall features, or from password management software. Putting certificates on a device or enabling a firewall feature does not certify identities or issue certificates; those are about storage or network protection, not issuing trusted attestations.

4. DDoS attacks are Attacks that utilize multiple systems to disrupt the traffic of a targeted systems by flooding the target with too much information in order to slow or crash the intended target(s).

A. Attacks that utilize multiple systems to disrupt the traffic of a targeted systems by flooding the target with too much information in order to slow or crash the intended target(s).

B. A method of data exfiltration

C. A technique to secure networks

D. A form of malware

DDoS is all about making a service unavailable by flooding it with traffic from many different sources. The statement describes exactly that: attacks that use multiple systems to overwhelm a target, consuming so much bandwidth and server capacity that legitimate requests can't get through. Because the attack comes from numerous machines, it's difficult to defend against with a single filter and is aimed at disabling services rather than stealing data or modifying information. This differs from data exfiltration, which focuses on secretly extracting data from a system. It also isn't a method for securing networks, which is about protection and defense, nor is it itself malware, which is software designed to perform harmful actions. (Note: some DDoS campaigns may utilize malware-infected devices to participate, but the attack type is defined by the coordinated flooding itself, not by being a form of malware.)

5. PKI is described as a framework.

A. True

B. False

C. It depends

D. Not sure

PKI is described as a framework because it isn't a single tool or protocol, but an integrated structure of roles, policies, standards, and components that together enable trusted use of public-key cryptography. It defines how keys are issued and managed, how identities are verified, how certificates are stored, distributed, and revoked, and how trust is extended through a system via entities like certificate authorities, registration authorities, certificate repositories, and revocation lists. This architecture supports authentication, data integrity, confidentiality, and non-repudiation across networks and applications. So describing PKI as a framework captures its role as an overarching system rather than a standalone product.

6. CTO is an acronym in DoD cyber policy. What does CTO stand for?

A. Cyber Tasking Order

B. Cyber Technical Operation

C. Cyber Tasking Oversight

D. Critical Task Order

In DoD cyber policy, a Cyber Tasking Order is the formal directive that assigns and directs specific cyber tasks to be carried out, with clear objectives, authorities, and timelines. This naming convention centers on the act of commanding actions in the cyber domain, making it the right term for an official instruction to perform cyber actions. The other options describe either the action itself (a cyber operation), the governance or oversight role, or a nonstandard term that isn't used as an official DoD designation, so they don't fit as the formal acronym in policy documents. For example, a Cyber Tasking Order would specify what needs to be done, by whom, and by when, enabling accountability and coordinated execution.

7. Which unit is responsible for executing DODIN and DCO operations?

A. Marine Corps Cyberspace Operations Group (MCCOG)

B. DISA

C. NSA

D. USCYBERCOM

The task being tested is who actually carries out defense and operations on the DoD Information Network, i.e., DODIN and Defensive Cyberspace Operations. In the Marine Corps, the unit tasked with executing those tasks is the Marine Corps Cyberspace Operations Group. They are the hands-on component that plans, defends, and conducts DCO activities on the DoD network for the Marine Corps, working under MARFORCYBER and in coordination with higher DoD authorities like DISA and USCYBERCOM. DISA provides the DoDIN infrastructure and security services at the DoD level rather than the Marine Corps' on-the-ground execution role. NSA handles intelligence-related work, not primary execution of DoDIN/DCO within a service. USCYBERCOM is the combatant command that directs cyber operations across the DoD, but the actual execution for the Marine Corps is carried out by MCCOG as the service-level component.

8. Critical Infrastructure security refers to which of the following?

A. The physical and cyber systems that are vital to the United States

B. Only government networks

C. Individual personal devices

D. Cloud service configurations

Critical Infrastructure security focuses on protecting the physical and cyber systems that are vital to the United States. This includes essential networks and assets like the power grid, water supply, transportation systems, hospitals, financial services, and communications, whose reliable operation is necessary for safety, security, and economic stability. The idea is to safeguard both the tangible infrastructure and the digital systems that control or connect it, so disruptions don't cascade into widespread harm. This broad view goes beyond just government networks, personal devices, or cloud configurations alone, since the threat landscape and resilience needs span all these interconnected systems that society depends on.

9. Which of the following is a countermeasure related to access control?

A. Biometric authentication systems

B. Phishing emails

C. Unencrypted data transfer

D. Public Wi-Fi access

The main idea being tested is how to enforce that only authorized people can reach resources. Biometric authentication systems are a strong countermeasure for access control because they verify identity using unique physical characteristics, such as fingerprints or facial features. This ties access to something inherent to the user, making it harder for someone else to impersonate you and enabling use as part of multi-factor authentication for additional protection. In practice, this helps ensure that granted access is truly to the right person, not just to someone who knows a password. Phishing emails, on the other hand, are a social engineering tactic that tries to steal credentials or trick users into revealing sensitive information; they don't provide a direct mechanism to control who can access a system. Unencrypted data transfer creates risks of interception and exposure but does not restrict access itself. Public Wi Fi access describes a network condition that can introduce risk or exposure rather than offer a way to enforce who is allowed in.

10. Which mechanism records user actions for auditing?

A. Authentication

B. Auditing

C. Accounting

D. Authorization

Understanding how actions are tracked for later review hinges on keeping a detailed record of who did what, when, and on which resources. This is what accounting provides: logs of user actions and resource usage that create an audit trail for accountability, billing, and compliance. Authentication is about proving identity, authorization governs access rights, and auditing is the process of examining logs. But the mechanism that actually records those actions to enable reviews and investigations is accounting.

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!