DSAC Annex F Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

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. What term describes voice features within IP technology such as voice calls and voicemail?

A. VoIP

B. PSTN

C. VPN

D. SIP

2. What is described as a top cybersecurity challenge?

A. The evolving nature of security risks as new technologies emerge

B. Overprovisioned security budgets

C. Too little data privacy regulation

D. Excessively centralized management

3. Which tool is supported by Cisco Extended Functions Service?

A. Quality Report Tool (QRT)

B. Security Dashboard

C. Vulnerability Scanner

D. Incident Console

4. PKI is described as a framework.

A. True

B. False

C. It depends

D. Not sure

5. Which HBSS component provides a secure communication channel to the ePO and manages all of the other modules?

A. HBSS

B. The McAfee Agent

C. ePO Console

D. Policy Auditor

6. Cybersecurity protects internet-connected systems from which of the following?

- **A. Cyber threats**
- **B. Bad weather**
- **C. Power outages**
- **D. Physical theft**

7. 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**

8. Advanced Persistent Threats (APTs) are best described as

- **A. Prolonged targeted attacks in which an attacker infiltrates a network and remains undetected for long periods of time with the aim to steal data.**
- **B. Brief automated scans for phishing.**
- **C. Random insider threats that steal hardware.**
- **D. Widespread malware that encrypts data for ransom.**

9. HBSS major components are listed as which of the following?

- **A. The Server, The Orchestrator Server, The McAfee Agent, The distributed repositories, The registered servers**
- **B. The Server, The Client, The Manager, The Database**
- **C. The Server, The Gateway, The Sensor, The Console**
- **D. The Server, The Orchestrator, The Agent, The Repository**

10. 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**

Answers

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

Explanations

1. What term describes voice features within IP technology such as voice calls and voicemail?

A. VoIP

B. PSTN

C. VPN

D. SIP

Voice over IP, or VoIP, is the term for delivering voice services over IP networks. It enables voice calls and voicemail by converting audio into data packets that travel over the same network used for data, integrating voice into the IP-based system. The other options don't describe the overall voice feature set: PSTN refers to the traditional telephone network that uses circuit switching; VPN is about creating secure connections over a network and isn't specific to voice features; SIP is a signaling protocol used to set up, manage, and terminate VoIP sessions, not the general label for IP-based voice services. So VoIP best captures voice features within IP technology.

2. What is described as a top cybersecurity challenge?

A. The evolving nature of security risks as new technologies emerge

B. Overprovisioned security budgets

C. Too little data privacy regulation

D. Excessively centralized management

The evolving nature of security risks as new technologies emerge stands out because the threat landscape doesn't stay still. As organizations adopt cloud services, IoT devices, AI-driven tools, mobile workforces, and increasingly complex supply chains, new ways to attack systems appear, and attackers continuously adapt their methods. This means defenses must be constantly updated, refreshed with fresh threat intelligence, and designed to anticipate emerging attack vectors rather than relying on static controls. Patches, configurations, access controls, and incident response plans all need ongoing refinement to keep pace with what attackers are doing today and likely to do tomorrow. That persistent, dynamic pressure—the need to evolve defenses in step with technology and threat actors—makes this the overarching challenge in cybersecurity. While budgets, regulation, and management structure matter, they don't capture the ongoing, universal pressure of changing risks driven by technology adoption.

3. Which tool is supported by Cisco Extended Functions Service?

A. Quality Report Tool (QRT)

B. Security Dashboard

C. Vulnerability Scanner

D. Incident Console

Cisco Extended Functions Service is designed to extend reporting capabilities by integrating with a tool that generates standardized quality metrics. The Quality Report Tool is the one that fits this role, providing structured reports on service quality and performance that EFS can surface for customers. The other tools—Security Dashboard, Vulnerability Scanner, and Incident Console—belong to different security or IT operations functions and aren't the tools specified as supported by EFS in this context. So the Quality Report Tool is the tool that EFS supports.

4. 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.

5. Which HBSS component provides a secure communication channel to the ePO and manages all of the other modules?

A. HBSS

B. The McAfee Agent

C. ePO Console

D. Policy Auditor

The key idea is how the endpoint is connected to and controlled by the central management system. The McAfee Agent sits on each protected machine and establishes a secure, authenticated channel to the ePolicy Orchestrator (ePO) server. Through this secure link, it receives policy updates, tasks, and configuration from ePO, and then enforces those instructions locally. In effect, this agent coordinates the operation of all the other HBSS modules on the endpoint, acting as the central control point that both communicates with ePO and drives how the other components behave. The ePO Console is the management interface, not the secure channel itself, and Policy Auditor is a separate module used for auditing policies rather than handling communication or coordination.

6. Cybersecurity protects internet-connected systems from which of the following?

A. Cyber threats

B. Bad weather

C. Power outages

D. Physical theft

Cybersecurity focuses on safeguarding internet-connected systems from digital threats carried out over networks. It aims to prevent attacks like malware, hacking attempts, phishing, ransomware, and other methods that try to access, alter, or disable data and services. This protection targets the online realm and the ways systems communicate and exchange information, helping keep data confidential, maintain integrity, and ensure availability even when attackers try to disrupt or breach them. The other options relate to non-digital risks: bad weather can disrupt operations but isn't something cybersecurity prevents directly; power outages involve energy reliability and continuity planning; physical theft concerns securing hardware and facilities rather than defending digital systems from online threats. So the risk cybersecurity is designed to mitigate is cyber threats.

7. 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.

8. Advanced Persistent Threats (APTs) are best described as

A. Prolonged targeted attacks in which an attacker infiltrates a network and remains undetected for long periods of time with the aim to steal data.

B. Brief automated scans for phishing.

C. Random insider threats that steal hardware.

D. Widespread malware that encrypts data for ransom.

APTs are campaigns where attackers use sophisticated techniques to break into a specific organization and stay hidden for a long time, quietly moving through the network to access sensitive data. The key idea is persistence and stealth: the attackers maintain a foothold, operate over extended periods, and avoid detection while they exfiltrate valuable information. This combination of targeted scope, long duration, and data-focused objectives best matches the description of prolonged, undetected access with a data theft goal. Other threat ideas described—brief automated phishing scans, insider threats, or widespread ransomware—do not capture the sustained, targeted, covert nature and data theft focus that defines Advanced Persistent Threats.

9. HBSS major components are listed as which of the following?

A. The Server, The Orchestrator Server, The McAfee Agent, The distributed repositories, The registered servers

B. The Server, The Client, The Manager, The Database

C. The Server, The Gateway, The Sensor, The Console

D. The Server, The Orchestrator, The Agent, The Repository

HBSS is built around a centralized management framework that ties together a server, orchestration, an endpoint agent, content repositories, and enrolled servers. The Server is the central hub for configuration, policy, and visibility. The Orchestrator Server handles automated tasks and workflow coordination across the environment. The McAfee Agent runs on each protected device, enforcing policies, reporting status, and pulling updates. Distributed repositories store and distribute content such as updates and signatures to streamline delivery. Registered servers are the HBSS-managed servers that have been enrolled to be controlled and monitored from the console. This combination reflects the key pieces that make HBSS operate as a coordinated security management system.

10. 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.

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!