DSAC Annex F Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

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. The statement “Security functions by pairing one public with another to authenticate users” is:

   A. False

   B. True

   C. Both true and false

   D. Not enough information

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

   A. VoIP

   B. PSTN

   C. VPN

   D. SIP

3. What does a Host-Based Intrusion Detection System (HIDS) do?

   A. A system that monitors the computer on which it is installed to detect an intrusion and logs the activity and notifies the designated authority

   B. A system that only scans network traffic

   C. A tool for encrypting disk drives

   D. A device that blocks all inbound connections by default

4. Which term best describes voice communications over an IP network?

   A. VoIP

   B. PSTN

   C. ISDN

   D. PBX

5. Digital certificates are typically issued and signed by:

   A. Certificate Authority

   B. Certificate Repository

   C. Security Center

   D. Key History

6. End User security involves measures taken to protect which of the following?

   A. Users, as well as their assets and information

   B. Only data in transit

   C. Only network devices

   D. Only administrators

7. What is Network security?

   A. Measures for protecting a computer network from intruders, including both wired and wireless connections.

   B. The practice of securing a single computer.

   C. The process of backing up data to the cloud.

   D. The management of user credentials.

8. PKI is described as a framework.

   A. True

   B. False

   C. It depends

   D. Not sure

9. Key History functionality includes:

   A. Storing certificate information to allow use of older keys

   B. Generating new keys on demand

   C. Reverting to older system policies

   D. Tracking login attempts

10. The HBSS major components include five items. Which system uses these five items as major components?

   A. HBSS

   B. HIDS

   C. VoIP

   D. QRT

Answers

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

Explanations

1. The statement “Security functions by pairing one public with another to authenticate users” is:

A. False

B. True

C. Both true and false

D. Not enough information

Authentication with public-key cryptography uses a key pair: a private key kept secret and a public key shared openly. You prove you own the private key by signing or decrypting data that the public key can verify. Pairing two public keys wouldn’t establish identity because nothing secret is demonstrated, since both keys are public. So the statement is false—the correct idea is pairing a private key with a public key to authenticate.

2. 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.

3. What does a Host-Based Intrusion Detection System (HIDS) do?

A. A system that monitors the computer on which it is installed to detect an intrusion and logs the activity and notifies the designated authority

B. A system that only scans network traffic

C. A tool for encrypting disk drives

D. A device that blocks all inbound connections by default

A Host-Based Intrusion Detection System focuses on the device it runs on, monitoring the host’s internal activity to spot signs of intrusion. It watches things like system logs, file changes, process behavior, and authentication events, looking for known attack patterns or unusual behavior. When something suspicious is detected, it logs evidence and sends an alert to the designated security authority so a response can be initiated. This host-level perspective is different from monitoring network traffic alone, which is what network-based IDS does, and from tools that encrypt data or block traffic by default, which don’t continuously monitor for intrusions on the host itself. So, monitoring the computer, logging activity, and notifying the appropriate response channel best captures what a HIDS does.

4. Which term best describes voice communications over an IP network?

A. VoIP

B. PSTN

C. ISDN

D. PBX

Voice communications over an IP network is described by VoIP, because VoIP specifically means sending speech as data packets over Internet Protocol networks. It involves converting voice into packets, using signaling to set up calls (such as SIP or H.323), and delivering the audio with protocols like RTP. This approach lets calls travel over the same networks that carry data, whether on the public internet or a private corporate network, often reducing costs and enabling easier integration with other IP-based services. By comparison, the traditional PSTN is the old circuit-switched public telephone network, ISDN is digital but still relies on circuit-switched channels, and PBX refers to a private branch exchange system for routing calls—not a term that describes voice over IP itself.

5. Digital certificates are typically issued and signed by:

A. Certificate Authority

B. Certificate Repository

C. Security Center

D. Key History

Digital certificates are part of a system that binds a public key to a verified identity, and the trusted issuer that does the binding is the certificate authority. The certificate authority issues certificates and signs them with its private key, creating a verifiable link between the identity and the public key. When a certificate is presented, others can verify the signature using the CA’s public key, which is trusted because the CA’s certificate is included in browsers and operating systems. Sometimes there are intermediate authorities that bridge to a root CA, but the core idea remains: a certificate is issued and signed by a certificate authority. Storing certificates in a repository doesn’t create or sign them, a security center isn’t the standard PKI role, and key history is about past keys, not issuing certificates.

6. End User security involves measures taken to protect which of the following?

A. Users, as well as their assets and information

B. Only data in transit

C. Only network devices

D. Only administrators

End user security focuses on safeguarding people and everything they interact with—their devices, accounts, data, and the actions they take. Because users can be targeted through phishing, weak passwords, or unsafe behaviors, the protections must cover the person and all their assets: user credentials, the devices they use (laptops, phones, tablets), the data they create or access, and the ways they access systems. That means implementing strong authentication, device protection, data encryption, access controls, and ongoing user education so individuals can recognize threats and act securely. While data in transit, network devices, or administrators have their own importance, end user security is about the broader picture of protecting the user and everything tied to them.

7. What is Network security?

A. Measures for protecting a computer network from intruders, including both wired and wireless connections.

B. The practice of securing a single computer.

C. The process of backing up data to the cloud.

D. The management of user credentials.

Network security is the set of measures that protect a computer network from intruders, covering both wired and wireless connections. It involves safeguarding the devices that make up the network (like routers, switches, and wireless access points), protecting data as it moves across the network, and controlling who can access network resources. Techniques such as firewalls, encryption, secure configurations, authentication and access controls, intrusion detection and prevention systems, and continuous monitoring work together to prevent unauthorized access, data theft, and service disruption. The aim is to secure the network as a whole, not just individual machines. Think of it as safeguarding the pathways and devices that let computers talk to each other and share information, rather than only protecting a single computer. For contrast, protecting a single computer is endpoint security, backing up data to the cloud is data protection and disaster recovery, and managing user credentials is identity and access management.

8. 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.

9. Key History functionality includes:

A. Storing certificate information to allow use of older keys

B. Generating new keys on demand

C. Reverting to older system policies

D. Tracking login attempts

Key History functionality focuses on maintaining a record of previously used keys and certificates so the system can still work with data protected by older keys. This is crucial during key rotation or certificate updates, because you may need to verify signatures or decrypt data that was created with past keys. By storing certificate information and the associated keys in history, the system can provide continuity, enable audits, and ensure access to legacy communications or documents without forcing immediate, permanent changes. That’s why storing certificate information to allow use of older keys is the best fit. It directly supports cryptographic agility and operational continuity across key lifecycles. Generating new keys on demand is about producing fresh keys rather than keeping track of past ones. Reverting to older system policies relates to policy versions, not cryptographic history. Tracking login attempts deals with authentication activity, not key history.

10. The HBSS major components include five items. Which system uses these five items as major components?

A. HBSS

B. HIDS

C. VoIP

D. QRT

HBSS is an integrated host-based security system built around five major components that work together on endpoints. Those parts provide centralized management, the agent installed on each host, the detection/prevention capabilities at the host level, auditing and compliance verification, and change/asset management to enforce configuration control. Because HBSS is defined by having these five components as its backbone, it is the system that uses them as its major components. The other options describe different concepts or systems (a generic host-based security approach, a voice communication system, or an incident response team) and do not match the five-part HBSS architecture.

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!