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

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. **Data Loss Prevention (DLP) focuses on preventing unauthorized access to sensitive data.**

   A. True

   B. False

   C. It depends

   D. Not sure

2. **Which security domain focuses on protecting information and assets from physical actions and events?**

   A. Physical security

   B. End User security

   C. Availability

   D. Integrity

3. **Which are key components of a System Security Plan (SSP) for Annex F?**

   A. System description, architecture, boundary, roles, controls, procedures, and assessment results.

   B. System description only and a list of hardware.

   C. Mission statement and marketing plan.

   D. Budget and procurement records.

4. **What does continuous verification imply in access control under Annex F?**

   A. Verification only at initial login

   B. Verification at every access attempt

   C. Verification only after a security event

   D. Verification during maintenance windows

5. **The technique that criminals use to attack users with targeted emails and fraudulent links is known as sphere fishing.**

   A. True

   B. False

   C. It depends

   D. Not sure

6. 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.

7. Which term describes measures that protect a computer network from intruders, including both wired and wireless connections?

A. Network security

B. Malware

C. Phishing

D. DDoS

8. Spear Phishing targets a specific individual or organization.

A. It has an intended target user, organization or business.

B. It targets a broad audience

C. It is delivered only by phone calls

D. It does not use emails

9. How should patch management be implemented to align with Annex F?

A. Patch strategy should be managed on a monthly basis with no testing.

B. Patches should be deployed only after approval.

C. Timely identification and deployment of critical patches, testing, rollback plan, and evidence of compliance.

D. Patches should be avoided.

10. What is the concept of risk acceptance and risk transference as described in Annex F?

A. Acceptance means no action due to low risk; transference uses insurance or outsourcing to shift risk.

B. Acceptance means buying insurance.

C. Transference means avoiding risk entirely.

D. Both are equivalent to data minimization.

Answers

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

Explanations

1. Data Loss Prevention (DLP) focuses on preventing unauthorized access to sensitive data.

A. True

B. False

C. It depends

D. Not sure

Data Loss Prevention is about stopping sensitive information from being exposed to people who shouldn't see it. It works by classifying data and then applying controls across data in use, in transit, and at rest—blocking risky actions, alerting on policy violations, and often encrypting or quarantining data to prevent leakage. Because preventing access by unauthorized parties is a fundamental way data can be lost or leaked, DLP's purpose includes stopping such access. In practice, DLP policies help ensure sensitive data isn't copied, emailed, uploaded, or shared with outsiders or with insiders who aren't authorized, so the statement aligns with what DLP tries to achieve.

2. Which security domain focuses on protecting information and assets from physical actions and events?

A. Physical security

B. End User security

C. Availability

D. Integrity

Physical security protects information and assets from physical actions and events by controlling access to facilities, rooms, and equipment, and by safeguarding the surrounding environment. This means using locks, fences, surveillance, badge access, and secure server rooms, as well as protecting backup media and data centers with fire suppression, climate control, and disaster-preparedness plans. By preventing unauthorized physical access and mitigating hazards like theft, vandalism, fire, floods, and power outages, it helps keep hardware and the data on it safe, preserving confidentiality and availability at the physical level. End User security focuses on how people interact with systems and devices; Availability is about ensuring systems and services are reachable when needed; Integrity concerns data being accurate and unaltered. While these areas matter, they address non-physical threats or data quality rather than protecting the physical space and equipment.

3. Which are key components of a System Security Plan (SSP) for Annex F?

A. System description, architecture, boundary, roles, controls, procedures, and assessment results.

B. System description only and a list of hardware.

C. Mission statement and marketing plan.

D. Budget and procurement records.

The key idea here is that a System Security Plan for Annex F should present a complete view of how the system is protected and how that protection is verified. The best answer includes all the essential elements that describe the system and the security measures around it. A System Security Plan should start with a thorough system description to establish what the system is, its purpose, and its major components. It then maps out the architecture and boundary, showing how the system is structured and what lies inside or outside its perimeters, which is crucial for understanding where risks may arise and what protections are needed at interfaces. Defining roles and responsibilities is next, so there is clear accountability for security tasks and decision-making. The plan also spells out the security controls chosen to protect the system, detailing how each control is implemented and maintained through specific procedures. Finally, assessment results provide evidence of how well the controls work, including test findings, remediation steps, and the current status of residual risk. This combination of description, structure, responsibilities, implemented controls with procedures, and ongoing assessment creates a living document that supports risk management, authorization, and continuous monitoring. Other options fall short because they omit essential security elements, such as the actual controls, procedures, and assessment evidence, or they focus on topics unrelated to security planning like mission statements, marketing plans, budgets, or procurement records.

4. What does continuous verification imply in access control under Annex F?

A. Verification only at initial login

B. Verification at every access attempt

C. Verification only after a security event

D. Verification during maintenance windows

Continuous verification in access control means validating the user's identity and their permissions at every attempt to access a resource, not just when they first log in. In Annex F, this approach ensures that access decisions reflect current conditions—if a user's rights are revoked, their device posture changes, or the context of the access shifts, the system can enforce the updated policy immediately on the next access attempt rather than relying on a one-time check. This reduces the risk of access lingering after changes and supports dynamic, least-privilege enforcement. Verifying only at initial login misses ongoing changes in authorization; verification only after a security event is reactive and allows a window of potential misuse; verification during maintenance windows is limited to those special periods and doesn't cover normal operation.

5. The technique that criminals use to attack users with targeted emails and fraudulent links is known as sphere fishing.

A. True

B. False

C. It depends

D. Not sure

Spear phishing is the targeted form of phishing where attackers research a specific person or organization and craft convincing emails with fraudulent links or attachments to steal credentials or deliver malware. The phrase "sphere fishing" isn't a recognized cybersecurity term, so the statement isn't accurate. Recognizing spear phishing involves looking for telltale signs like personalization that seems off, mismatched or suspicious sender details, urgent language pressuring you to act, and links that don't match the legitimate site even if they look similar at a glance. Defenses include verifying the sender, hovering over links to inspect the actual URL before clicking, enabling multi-factor authentication, and relying on training and email filtering to catch deceptive messages.

6. 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.

7. Which term describes measures that protect a computer network from intruders, including both wired and wireless connections?

A. Network security

B. Malware

C. Phishing

D. DDoS

Network security is the set of measures designed to protect a computer network from intruders and threats, for both wired and wireless connections. It combines policies and technical controls—firewalls that filter traffic, intrusion detection systems that watch for suspicious activity, encryption to keep data in transit private, strong authentication and access controls, secure configurations, and regular patching and network segmentation. For wireless networks, it also includes protections like robust Wi Fi encryption (such as WPA3), proper authentication, and safeguards against rogue access points. The other terms point to specific threats or attack methods: malware is harmful software, phishing is a social engineering tactic to steal credentials, and DDoS is an attack that overwhelms services with traffic. Network security, in contrast, is about preventing intrusions across both wired and wireless paths.

8. Spear Phishing targets a specific individual or organization.

A. It has an intended target user, organization or business.

B. It targets a broad audience

C. It is delivered only by phone calls

D. It does not use emails

Spear phishing hinges on targeting a specific person or organization with a crafted, credible message. The attacker researches the target and uses details about their role, workplace, or relationships to impersonate someone trusted or to reference familiar events, making the communication feel legitimate. Because the aim is to deceive a particular individual or entity, the approach is distinguished from broad phishing that targets many people with generic content. While email is a common delivery method for spear phishing, the defining trait is the intentional focus on a single target or narrow group, not the delivery channel itself. That emphasis on a targeted target is what makes this option the best match.

9. How should patch management be implemented to align with Annex F?

A. Patch strategy should be managed on a monthly basis with no testing.

B. Patches should be deployed only after approval.

C. Timely identification and deployment of critical patches, testing, rollback plan, and evidence of compliance.

D. Patches should be avoided.

The essential idea here is that patch management must be proactive and controlled to reduce risk, with a clear lifecycle that includes timely action, verification, and evidence for audits. The best option emphasizes identifying critical patches quickly, deploying them promptly, testing before broad rollout to avoid breaking systems, having a rollback plan if something goes wrong, and keeping evidence of compliance. This combination ensures vulnerabilities are remediated fast while preserving stability and providing auditable proof that controls are in place and functioning. Patching only on a monthly schedule without testing leaves gaps and uncertainty about compatibility, defeating the goal of safe, timely remediation. Relying on approvals alone can introduce delays and does not guarantee the patches are actually applied when needed. Avoiding patches entirely is contrary to any security standard.

10. What is the concept of risk acceptance and risk transference as described in Annex F?

A. Acceptance means no action due to low risk; transference uses insurance or outsourcing to shift risk.

B. Acceptance means buying insurance.

C. Transference means avoiding risk entirely.

D. Both are equivalent to data minimization.

Risk acceptance is when you decide not to take action to reduce a risk because it falls within your tolerance, while risk transference moves the potential impact to someone else—typically through insurance or outsourcing arrangements. The best answer captures this: acceptance means no action is taken due to low risk, and transference shifts risk to a third party via insurance or outsourcing. Buying insurance is a form of transference, not acceptance, and transference does not eliminate risk entirely. Data minimization is a separate concept and not the same as these approaches.

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!