# DSAC-11 Annex B 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 number of flash cards was proposed in the alternative plan?**

   **A. 50**

   **B. 25**

   **C. 75**

   **D. 100**

2. **Which access control model assigns access by owner discretion?**

   **A. Discretionary Access Control**

   **B. Mandatory Access Control**

   **C. Attribute-Based Access Control**

   **D. Role-Based Access Control**

3. **What is the purpose of limiting access to Control Panel through Group Policy?**

   **A. To prevent unauthorized access to sensitive system settings**

   **B. To prevent users from changing wallpaper**

   **C. To reduce startup time**

   **D. To ensure faster network logins**

4. **What is an incident response plan and its typical phases for Annex B?**

   **A. A documented process for detecting, responding to, recovering from security incidents; phases include preparation, detection, containment, eradication, recovery, lessons learned.**

   **B. A plan to manage marketing incidents.**

   **C. A plan for hardware replacement only.**

   **D. A plan to ignore incidents.**

5. **The operating system acts as the interface between the user and the hardware. True or False?**

   **A. True**

   **B. False**

   **C. Not sure**

   **D. Not applicable**

**6. Which DSAC domain focuses on responding to security incidents?**

**A. Governance**

**B. Network Security**

**C. Incident Response**

**D. Software Assurance**

**7. In STRIDE threat modeling, which category covers risks where an attacker can perform actions with more privileges than allowed?**

**A. Spoofing**

**B. Tampering**

**C. Repudiation**

**D. Elevation of Privilege**

**8. In an incident response plan, which phase focuses on analyzing the incident after recovery to improve future responses?**

**A. Preparation**

**B. Containment**

**C. Recovery**

**D. Lessons Learned**

**9. Which measures protect logging integrity in Annex B?**

**A. Regular log rotation and deletion to save space.**

**B. Centralized storage of logs.**

**C. Write-once or tamper-evident logs, centralized storage, and cryptographic signing.**

**D. Logs stored locally on user devices only.**

**10. Which statement best describes red team and blue team activities in security testing?**

**A. Blue team conducts simulated attacks to breach defenses.**

**B. Red team only observes without interacting.**

**C. Blue team handles incident response during normal operation.**

**D. Red team attempts to breach the system; blue team defends, detects, and responds to findings.**

# Answers

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

# Explanations

## 1. What number of flash cards was proposed in the alternative plan?

**A. 50**

**B. 25**

**C. 75**

**D. 100**

**The number of flash cards in a study plan is about balancing coverage with mental effort. Choosing a moderate deck size—the middle option among the four—tends to work best because it covers essential material without overwhelming you. With a manageable set, you can review more frequently, practice retrieval, and reinforce memory through spaced repetition, which strengthens long-term retention. If you go with too few cards, you risk missing important topics and leaving gaps in your understanding. If you push for too many, daily review can feel daunting, reducing consistency and weakening the quality of practice. The middle choice hits a sweet spot: it's large enough to touch on key areas, yet small enough to keep sessions focused and sustainable over time.**

## 2. Which access control model assigns access by owner discretion?

**A. Discretionary Access Control**

**B. Mandatory Access Control**

**C. Attribute-Based Access Control**

**D. Role-Based Access Control**

**Discretionary access control is the model where the owner of a resource decides who can access it and what actions they may perform. In this approach, the owner can set and change permissions—typically using mechanisms like access control lists or capability tokens attached to the resource. This contrasts with other models: mandatory access control enforces system-wide policies set by an administrator and is not about the owner's choices; attribute-based access control grants access based on user, resource, and environmental attributes; and role-based access control assigns permissions according to predefined roles rather than individual ownership. So, when the emphasis is on owner discretion to grant or revoke access, discretionary access control is the best fit.**

## 3. What is the purpose of limiting access to Control Panel through Group Policy?

**A. To prevent unauthorized access to sensitive system settings**

**B. To prevent users from changing wallpaper**

**C. To reduce startup time**

**D. To ensure faster network logins**

**Limiting access to the Control Panel through Group Policy is about protecting configuration by preventing users from viewing or changing settings that can affect the machine's security and stability. With Group Policy, an administrator can hide or disable Control Panel applets or restrict which settings a user can modify, ensuring that only authorized personnel can adjust critical options. This helps maintain a consistent, secure baseline and reduces the risk of accidental or intentional misconfiguration. Other options don't capture that intent. Changing wallpaper is a cosmetic setting and not about safeguarding system configuration. Startup time and network logon speed aren't directly influenced by restricting Control Panel access.**

## 4. What is an incident response plan and its typical phases for Annex B?

**A. A documented process for detecting, responding to, recovering from security incidents; phases include preparation, detection, containment, eradication, recovery, lessons learned.**

**B. A plan to manage marketing incidents.**

**C. A plan for hardware replacement only.**

**D. A plan to ignore incidents.**

**An incident response plan is a documented process for detecting, responding to, and recovering from security incidents, providing a structured approach so teams know what to do, who to contact, and how to restore operations while preserving evidence. The typical phases give that lifecycle a clear path: preparation sets up the team, tools, communication channels, and escalation criteria; detection and analysis involve monitoring, identifying incidents, and assessing their impact; containment aims to limit the spread and preserve evidence; eradication removes the root cause and cleans affected systems; recovery focuses on restoring services to normal and validating that systems are secure; and finally, lessons learned captures insights, updates to the plan, and actions to prevent recurrence. This framing explains why the option describing a comprehensive, documented process with these phases is the best choice. The other options describe things unrelated to incident response, such as marketing-related plans, hardware-only plans, or ignoring incidents, which do not provide a coordinated security response.**

## 5. The operating system acts as the interface between the user and the hardware. True or False?

**A. True**

**B. False**

**C. Not sure**

**D. Not applicable**

**The operating system serves as the interface between users (and their programs) and the computer hardware. It hides hardware details and offers a stable set of services—through system calls, libraries, and device drivers—that let applications perform tasks like input/output, memory access, and file management. The OS manages and coordinates hardware resources (CPU time, memory, I/O devices) so users can interact with the computer via a friendly interface (command line or GUI) and software can run without needing to control hardware directly. That separation is why the statement is true.**

## 6. Which DSAC domain focuses on responding to security incidents?

**A. Governance**

**B. Network Security**

**C. Incident Response**

**D. Software Assurance**

**Responding to security incidents is the focus of the DSAC domain called Incident Response. This domain covers what teams do when a security event is detected: preparing and planning for incidents, quickly identifying and analyzing what happened, containing the threat to prevent further damage, eradicating the cause, recovering normal operations, and reviewing the incident to improve defenses. It also emphasizes coordinating with IT staff, security operations, management, and, when needed, external partners or authorities to minimize impact and learn from the event. Other DSAC domains focus on different areas: Governance deals with policies, risk management, and compliance; Network Security concentrates on protecting the network and data in transit with controls like firewalls and monitoring; Software Assurance ensures software is secure by design and maintained securely through practices like secure coding and vulnerability management.**

## 7. In STRIDE threat modeling, which category covers risks where an attacker can perform actions with more privileges than allowed?

**A. Spoofing**

**B. Tampering**

**C. Repudiation**

**D. Elevation of Privilege**

**Elevation of Privilege is when an attacker gains higher access rights than they should have. In STRIDE, this category covers exploits that allow someone to perform actions that require more privileges than their authenticated role should permit, such as a standard user executing admin-level commands or accessing restricted data by exploiting a vulnerability or misconfiguration. This directly matches the idea of doing things with more privileges than allowed. It's different from spoofing (pretending to be someone else), tampering (modifying data), repudiation (dishing out or denying actions), or other threat types that don't involve increasing privilege. Preventing these threats relies on proper access control, least-privilege enforcement, and patching known vulnerabilities to close privilege-escalation paths.**

## 8. In an incident response plan, which phase focuses on analyzing the incident after recovery to improve future responses?

**A. Preparation**

**B. Containment**

**C. Recovery**

**D. Lessons Learned**

**The main idea tested is how we learn from an incident after things have been brought back to normal. This phase is about looking back at what happened, analyzing what went well and what didn't, and turning those insights into concrete improvements for the future. By conducting a post-incident review, you identify root causes, gaps in detection, delays in response, and communication or coordination issues. Then you update the incident response plans, runbooks, training, and controls so future incidents can be detected sooner, contained faster, and recovered more smoothly. Other phases focus on getting ready beforehand, stopping the incident from spreading, or restoring services, but the reflective work that feeds back into better preparedness and response is the lessons-learned phase.**

## 9. Which measures protect logging integrity in Annex B?

**A. Regular log rotation and deletion to save space.**

**B. Centralized storage of logs.**

**C. Write-once or tamper-evident logs, centralized storage, and cryptographic signing.**

**D. Logs stored locally on user devices only.**

**Protecting logging integrity means making sure logs are trustworthy, tamper-evident, and verifiable. The best option combines three ideas: write-once or tamper-evident storage so entries can't be altered without detection; centralized storage so there's a single, auditable repository with consistent security controls; and cryptographic signing to authenticate each log entry and prove it hasn't been changed. Together, these measures cover detection of tampering, trustworthy provenance, and an authoritative record that can be validated later. Rotating or deleting logs to save space can erase evidence and doesn't prevent or reveal tampering. Centralized storage helps with consistency and access control, but without tamper detection and signing, changes could go unnoticed. Storing logs only on local devices concentrates risk in a single device that could be compromised or lost, making them harder to verify and recover.**

**10. Which statement best describes red team and blue team activities in security testing?**

**A. Blue team conducts simulated attacks to breach defenses.**

**B. Red team only observes without interacting.**

**C. Blue team handles incident response during normal operation.**

**D. Red team attempts to breach the system; blue team defends, detects, and responds to findings.**

**Red team vs blue team dynamics in security testing involve an attacker-like simulation and a defender's response. The best statement captures the essence: the red team actively tries to breach the system, using techniques similar to real attackers, while the blue team defends, detects, and responds to the findings, closing gaps and improving defenses. This reflects how offensive tests reveal weaknesses and how defensive teams learn to recognize and mitigate threats, then adapt defenses and incident response plans accordingly. In practice, red team activities push defenses by attempting breaches, phishing, or exploitation within agreed rules of engagement, while blue team activities focus on monitoring, alerting, containment, eradication, and recovery to reduce risk. The other descriptions miss this critical interaction: one misattributes attacking to the blue team, another suggests red team only observes without interaction, and another partial statement doesn't fully capture the defender's active response to findings.**

# 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://dsac11annexb.examzify.com**

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