AFSC CYBERSPACE OPERATIONS OFFICER (17D) BLOCK 5 PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://adsc17dblock5.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

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

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 15

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. In addition to the base documents, which forms are required for hazardous cargo that is also sensitive?

A. DD 1387-2 and DD Form 1907

B. AMC Form 1033, DD 1387-2, and DD Form 1907

C. AMC Form 1033 only

D. DD Form 1907 only

2. Which functional area is A3?

A. Logistics

B. Communications

C. Operations

D. Strategic Plans & Programs

3. Which practice is part of hardening a Windows workstation?

A. Disable unnecessary services

B. Enable default guest account

C. Turn off updates

D. Disable firewall

4. Data Loss Prevention (DLP) techniques are typically applied to which areas?

A. Endpoints, email gateways, and cloud services.

B. Core routers only.

C. USB drives only.

D. Print servers only.

5. Which components are typically included in post-incident activities within a playbook?

A. Post-incident lessons learned and communication, among others.

B. Budget approval and vendor negotiation.

C. Marketing outreach after incident.

D. Physical security checks unrelated to incident.

SAMPLE

6. Which of the following is NOT one of the six steps in the Risk Management Framework (RMF) used to manage cyber risk for information systems?

A. Categorize

B. Select

C. Encrypt

D. Monitor

7. Which statement best describes the Master Station Log?

A. A log of weather data

B. A personnel roster

C. Time-based record of events used to maintain continuity and reporting

D. A financial ledger for deployments

8. How many copies of the packing list are required?

A. 6

B. 3

C. 4

D. 2

9. What can your unit do if you cannot meet the tasking requirement?

A. Substitution waiver, shortfalls, reclama

B. Substitution waiver only

C. Shortfalls only

D. Reclama only

10. What is MITRE ATT&CK for ICS and why is it relevant to 17D?

A. A knowledge base of attacker techniques for IT networks.

B. A set of guidelines for cloud adoption.

C. A vulnerability scoring system for general IT.

D. A knowledge base of attacker techniques specific to industrial control systems; relevant for defending critical infrastructure and ICS networks.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. In addition to the base documents, which forms are required for hazardous cargo that is also sensitive?

A. DD 1387-2 and DD Form 1907

B. AMC Form 1033, DD 1387-2, and DD Form 1907

C. AMC Form 1033 only

D. DD Form 1907 only

The main idea is that hazardous cargo that is also considered sensitive requires extra, specific documentation to ensure proper handling, accountability, and security. The three forms work together to cover these aspects: the hazard data form provides the critical details about the material's hazards, classification, packaging, and emergency information so handlers and carriers know exactly what they're dealing with and how to respond. The receiving report documents what was actually received, its condition, and serves as a traceable record for verification and discrepancy resolution. The authorization form ensures the shipment has been cleared and approved for movement, addressing security and custody requirements for sensitive items. Using all three forms together guarantees that the hazardous material is described and handled correctly, that there is a reliable record of receipt, and that the shipment is properly authorized for transport. Without any one of these, essential safety, accountability, or security elements would be missing. That's why including AMC Form 1033 along with DD 1387-2 and DD Form 1907, in addition to the base documents, is required for hazardous cargo that is also sensitive.

2. Which functional area is A3?

A. Logistics

B. Communications

C. Operations

D. Strategic Plans & Programs

A3 designates the Operations function. In the Air Force staff structure, this area is responsible for directing and controlling current air operations, mission execution, and coordinating actions to achieve operational objectives. The other options map to different areas: Logistics handles supply and sustainment, Communications covers command, control, and information systems, and Strategic Plans & Programs deals with long-range planning and program management. So, A3 being Operations is the best fit.

3. Which practice is part of hardening a Windows workstation?

A. Disable unnecessary services

B. Enable default guest account

C. Turn off updates

D. Disable firewall

Hardening a Windows workstation means reducing the attack surface by removing or disabling everything that isn't needed for the machine's role. Each running service is like an entry point potential attackers could abuse, so turning off unnecessary services minimizes the chances of exploits and misconfigurations, and can also free up system resources. That's why disabling unnecessary services is the best practice in this scenario. In contrast, enabling the default guest account creates a foothold for unauthorized access; turning off updates leaves the system open to known vulnerabilities; and disabling the firewall removes a critical defense that helps block unwanted network traffic.

SAMPLE

4. Data Loss Prevention (DLP) techniques are typically applied to which areas?

A. Endpoints, email gateways, and cloud services.

B. Core routers only.

C. USB drives only.

D. Print servers only.

DLP is about preventing sensitive information from leaving an organization by watching the main paths data travels and where it resides. The strongest coverage comes from protecting data on endpoints (where users create and copy data), at the email gateways (where data moves in and out via email), and in cloud services (where data is stored, shared, and collaborated on). Covering these three areas captures the primary leakage channels: data on user devices, data moving through email, and data stored or shared in the cloud. Limiting DLP to core routers would miss data on endpoints and in cloud storage. Focusing only on USB drives would overlook data flowing over networks and into cloud services. Restricting to print servers would miss the vast majority of modern data flows, especially email and cloud-based data.

5. Which components are typically included in post-incident activities within a playbook?

A. Post-incident lessons learned and communication, among others.

B. Budget approval and vendor negotiation.

C. Marketing outreach after incident.

D. Physical security checks unrelated to incident.

Post-incident activities in a playbook focus on turning what happened into actionable improvements: capturing lessons learned, documenting what occurred, and communicating findings to the right stakeholders. This phase ensures the team understands what worked, what didn't, and what needs to change, while also outlining follow-up actions, remediation steps, and updates to other playbooks or defenses. That combination—lessons learned and communication, along with the accompanying actions—is why this option is the best fit for post-incident work. Budget approval and vendor negotiation are typically part of planning or procurement processes rather than the immediate post-incident learning cycle. Marketing outreach after an incident isn't a standard post-incident playbook task, since the focus is on internal improvement and containment, not external messaging. Physical security checks unrelated to the incident fall outside the post-incident IT and cybersecurity response workflow and would be addressed separately.

6. Which of the following is NOT one of the six steps in the Risk Management Framework (RMF) used to manage cyber risk for information systems?

A. Categorize

B. Select

C. Encrypt

D. Monitor

The process being tested is the Risk Management Framework (RMF), a lifecycle used to manage cyber risk for information systems. It consists of six distinct steps: categorize the system and the data to determine impact levels, select the appropriate security controls, implement those controls, assess their effectiveness, authorize the system to operate, and continuously monitor the security state. Encryption is a security control technique that can be used within the implementation of controls or during assessment, but it is not itself a separate RMF step. Knowing the six-step flow helps you see that categorizing, selecting, and monitoring fit as steps, while encryption is a tool used within the framework rather than a standalone step.

SAMPLE

7. Which statement best describes the Master Station Log?

A. A log of weather data

B. A personnel roster

C. Time-based record of events used to maintain continuity and reporting

D. A financial ledger for deployments

The Master Station Log is a running, time-stamped record of events at the master station. It captures what happened, when it happened, and who or what was involved, creating a chronological narrative of transmissions, messages, equipment status, outages, and other significant actions. This time-based record is essential for maintaining continuity of operations—so anyone reviewing the log can reconstruct the sequence of events, understand why decisions were made, and prepare accurate reports or handoffs between shifts. It isn't simply weather data, a personnel roster, or a financial ledger, which is why the time-based narrative of events used for continuity and reporting is the best description.

8. How many copies of the packing list are required?

A. 6

B. 3

C. 4

D. 2

The main idea is that packing lists must be distributed to multiple people or offices to keep a complete, verifiable record as gear moves from departure to arrival. Requiring six copies ensures every relevant stakeholder has a current copy to compare against the actual contents, confirm items are present, and sign off at each stage. This creates a clear chain of accountability and makes audits or inspections straightforward. In practice, the six copies typically cover the traveler, the unit's operations or supervising office, the maintenance/QA liaison, the supply/stock control, the transportation or receiving point, and the unit's records. If you had fewer copies, some recipient would lack a record, increasing the risk of missing items or disputes. More than six adds unnecessary overhead beyond the standard process. So, six copies aligns with the established distribution for thorough accountability.

9. What can your unit do if you cannot meet the tasking requirement?

A. Substitution waiver, shortfalls, reclama

B. Substitution waiver only

C. Shortfalls only

D. Reclama only

When you can't meet a tasking, the key action is to clearly report the deficiency you're facing. This means identifying the shortfall—the exact capability, personnel, or resource gap—and communicating its impact, timing, and any preliminary mitigation ideas to the chain of command so they can decide on re-tasking, adjustment, or priority. The best choice captures that specific, actionable pathway: document and report the shortfall. Substitution waivers are a separate authority used to allow substituting a different asset or capability, but they aren't the immediate means to address an inability to meet the tasking on hand. Reclama (reclamation) isn't the direct mechanism for resolving a failure to satisfy a current tasking. Therefore, reporting shortfalls is the correct and primary action in this scenario.

SAMPLE

10. What is MITRE ATT&CK for ICS and why is it relevant to 17D?

A. A knowledge base of attacker techniques for IT networks.

B. A set of guidelines for cloud adoption.

C. A vulnerability scoring system for general IT.

D. A knowledge base of attacker techniques specific to industrial control systems; relevant for defending critical infrastructure and ICS networks.

MITRE ATT&CK for ICS is a knowledge base that catalogs attacker techniques specifically observed in industrial control system environments. It extends the general ATT&CK framework to reflect the unique devices, protocols, and safety constraints of ICS—think SCADA, PLCs, HIS/engineering workstations, and control networks—so defenders can map what adversaries do to concrete ICS contexts, detect those actions, and plan effective mitigations. This focused lens is especially valuable for 17D because defending critical infrastructure and ICS networks requires understanding how an attacker might operate within those systems, how they could move or manipulate control logic, and what observable signals those actions would produce. Using ATT&CK for ICS provides a common language for threat modeling, detection development, and defensive planning, helping prioritize protections and inform exercises and risk communications. In short, it's a knowledge base of attacker techniques specific to industrial control systems, highly relevant for safeguarding critical infrastructure and ICS networks.

SAMPLE

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://adsc17dblock5.examzify.com

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

SAMPLE