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

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 does MGRS stand for?

A. Military Grid Reference System

B. Master Grid Reference System

C. Military Geodetic Reference System

D. Magnitude Grid Reference System

2. Which statement correctly differentiates cyber threat intelligence (CTI) from broader cyber intelligence (CI) as used in operations?

A. CTI is the broader analysis; CI focuses specifically on threats.

B. CTI is specifically information about cyber threats, adversaries, and their TTPs; cyber intelligence is the broader analysis of adversaries and capabilities; CTI informs cyber planning and defense.

C. CTI and CI are identical concepts.

D. CTI only covers hardware vulnerabilities and not adversaries.

3. In the cyber kill chain model, which of the following is NOT a typical phase?

A. Reconnaissance

B. Delivery

C. Installation

D. Containment

4. Which are the NIST SP 800-53 control families cited as examples under Security and Privacy Controls?

A. Contingency Planning, Media Protection, and Identification and Authentication

B. Access Control, Audit and Accountability, and Configuration Management

C. Program Management, Risk Assessment, and Continuous Monitoring

D. Physical and Environmental Protection, System and Communications Protection, and Incident Response

5. Identify three relevant offices/positions concerning readiness and deployments.

A. IDO, IDRC, and DCC

B. IDO, IDRC, and UDM

C. PDF, CDF, and DCC

D. IDO, DCC, and PDF

6. Which NIST SP 800-53 control family is most directly associated with cyber defense?

A. System and Communications Protection.

B. Security and Privacy Controls for Information Systems and Organizations; e.g., controls in the Access Control, Audit and Accountability, and Configuration Management families.

C. Physical and Environmental Protection.

D. Program Management.

7. What are the primary steps in cyber risk management for an enterprise network?

A. Identify assets and threats, assess vulnerabilities and risk, implement controls and mitigations, and monitor and review risk.

B. Deploy more servers, hire more staff, and increase training budgets.

C. Ignore risk; patch only when required.

D. Risk management is only about compliance paperwork.

8. What are some of the events logged by the Master Station Log?

A. Weather events, Transportation logs, Vendor visits, Deployment start

B. Hardware setup/teardown, Network or service interruptions, project work, changeover, and status updates

C. User login times, Power usage, Cable runs, Maintenance windows

D. Security incidents, Equipment purchases, Training schedules, Changeover

9. What is the difference between incident response and incident handling in cyberspace operations?

A. Incident response is the overall process of detecting, containing, and recovering from an incident; incident handling is the day-to-day management and coordination.

B. Incident response is the network monitoring tool; incident handling is the firewall.

C. Incident response is only about reporting incidents; incident handling is about containment.

D. They are the same.

10. Describe the UDM.

A. Oversees security clearances

B. Manages maintenance schedules

C. Coordinates personnel relocations

D. Manages deployment readiness and training aspects for all deployable personnel and/or cargo within their unit

Answers

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

Explanations

1. What does MGRS stand for?

A. Military Grid Reference System

B. Master Grid Reference System

C. Military Geodetic Reference System

D. Magnitude Grid Reference System

MGRS stands for Military Grid Reference System. It's a standardized way the military uses to convey precise locations by turning latitude/longitude or UTM-like coordinates into a compact string. Built on the UTM and UPS coordinate ideas, MGRS adds a zone number, a latitude band, a 100-kilometer grid square designator, and then easting and northing values in meters. This structure lets personnel rapidly communicate exact positions over radio or in maps, with the level of detail determined by how many digits are used for the easting and northing. The other options don't fit because they describe different concepts or names that aren't used for this system. Master implies a single master system, which isn't how MGRS is defined; Geodetic refers to the broader science of measuring Earth and its coordinate systems, not this specific grid framework; Magnitude relates to size or intensity, not a coordinate reference system.

2. Which statement correctly differentiates cyber threat intelligence (CTI) from broader cyber intelligence (CI) as used in operations?

A. CTI is the broader analysis; CI focuses specifically on threats.

B. CTI is specifically information about cyber threats, adversaries, and their TTPs; cyber intelligence is the broader analysis of adversaries and capabilities; CTI informs cyber planning and defense.

C. CTI and CI are identical concepts.

D. CTI only covers hardware vulnerabilities and not adversaries.

The key idea is that cyber threat intelligence is the specific, actionable information about threats, adversaries, and their tactics, techniques, and procedures, which directly informs how you plan and defend your cyber environment. This specialized intelligence focuses on who is behind attacks, what they are capable of, and how they operate, so you can anticipate, detect, and counter their techniques. That makes the correct statement the best fit: cyber threat intelligence describes threats, adversaries, and their TTPs, and it feeds cyber planning and defense. Broad cyber intelligence, on the other hand, encompasses a wider set of analyses about adversaries and capabilities beyond just immediate threats, including other aspects of the cyber domain that aren't limited to threat information. The other options mischaracterize the relationship. It's not broader than CTI, not identical to CI, and not limited to hardware vulnerabilities without addressing adversaries.

3. In the cyber kill chain model, which of the following is NOT a typical phase?

A. Reconnaissance

B. Delivery

C. Installation

D. Containment

The cyber kill chain traces the attacker's progression from initial information gathering to achieving objectives. Typical stages include reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Containment is a defensive action taken to stop the attacker and limit damage after detection, not a step the attacker performs. Because the kill chain describes attacker actions, containment isn't considered a normal phase of the chain. Reconnaissance, delivery, and installation all represent concrete attacker activities: recon and weaponization precede delivery, which is followed by exploitation and installation to establish foothold.

4. Which are the NIST SP 800-53 control families cited as examples under Security and Privacy Controls?

A. Contingency Planning, Media Protection, and Identification and Authentication

B. Access Control, Audit and Accountability, and Configuration Management

C. Program Management, Risk Assessment, and Continuous Monitoring

D. Physical and Environmental Protection, System and Communications Protection, and Incident Response

NIST SP 800-53 groups controls into families, and Security and Privacy Controls examples point to three key families: Access Control, Audit and Accountability, and Configuration Management. Access Control covers who can access resources and what they can do; Audit and Accountability focuses on recording events and ensuring traceability of actions; Configuration Management ensures that system configurations are controlled, tracked, and kept in a secure baseline to prevent unauthorized changes. While other control families like Contingency Planning, Media Protection, or Program Management are important parts of the overall framework, the cited examples in that context are the three mentioned above.

5. Identify three relevant offices/positions concerning readiness and deployments.

A. IDO, IDRC, and DCC

B. IDO, IDRC, and UDM

C. PDF, CDF, and DCC

D. IDO, DCC, and PDF

The concept being tested is identifying the three offices that directly manage readiness and deployments at different levels of the Air Force structure. The three relevant offices are the Installation Deployment Officer, the Installation Deployment Readiness Center, and the Unit Deployment Manager. The Installation Deployment Officer serves at the base level to coordinate deployment actions and ensure airmen and units meet deployment requirements, acting as a primary point of contact for deployment policy and processes. The Installation Deployment Readiness Center is the hub that maintains visibility into readiness data, tracks personnel and equipment status, and produces readiness reports for leadership, helping to keep everyone informed about who can deploy and when. The Unit Deployment Manager works at the unit level to prepare individuals and teams for deployment—ensuring proper training, certifications, and equipment are in place, and managing deployment schedules and accountability. Together, these offices cover policy coordination, readiness tracking, and unit-level execution, which is why they form the correct trio for readiness and deployments.

6. Which NIST SP 800-53 control family is most directly associated with cyber defense?

A. System and Communications Protection.

B. Security and Privacy Controls for Information Systems and Organizations; e.g., controls in the Access Control, Audit and Accountability, and Configuration Management families.

C. Physical and Environmental Protection.

D. Program Management.

NIST SP 800-53 organizes controls into families that address different aspects of safeguarding information systems. For cyber defense, the most direct fit is the Security and Privacy Controls for Information Systems and Organizations family because it provides the comprehensive set of safeguards that defend the system and data in practice. This family includes essential technical and procedural controls such as access control (restricting who can use and reach systems), audit and accountability (logging and monitoring to detect, investigate, and respond to incidents), and configuration management (maintaining secure, consistent baselines to reduce exploitable weaknesses). These elements collectively support defensive operations by preventing unauthorized access, ensuring visibility into activity, and keeping systems in a secure, known state. In contrast, System and Communications Protection focuses more specifically on protecting communications and boundaries, which is a narrower aspect of defense. Physical and Environmental Protection covers non-technical risks tied to facilities, not the technical controls of cyber defense. Program Management deals with governance and organizational processes rather than direct technical safeguards. Therefore, the family that best aligns with cyber defense is the Security and Privacy Controls for Information Systems and Organizations family.

7. What are the primary steps in cyber risk management for an enterprise network?

A. Identify assets and threats, assess vulnerabilities and risk, implement controls and mitigations, and monitor and review risk.

B. Deploy more servers, hire more staff, and increase training budgets.

C. Ignore risk; patch only when required.

D. Risk management is only about compliance paperwork.

Cyber risk management in an enterprise network follows a lifecycle that starts with knowing what you have and what could threaten it, then assessing how exposed you are, putting in place protections, and continuously watching for changes. The first step is identifying assets and threats—take an inventory of critical systems, data, and services, and consider who or what might meaningfully threaten them (for example, adversaries, misconfigurations, or supply-chain risks). Next, assess vulnerabilities and risk by evaluating how likely those threats are to exploit weaknesses and what the potential impact would be on operations, data, and reputation. With that understanding, you implement controls and mitigations to reduce risk, which includes technical measures like patching, configuration management, access controls, and network segmentation, as well as administrative actions such as policies and training. Finally, you monitor and review risk on an ongoing basis, rechecking the asset landscape, updating risk scores, validating control effectiveness, and adjusting defenses as the environment or threat picture evolves. This continuous cycle aligns with established risk management practices and ensures protection adapts to changes rather than remaining static. The other approaches don't address this structured, ongoing process. Merely expanding resources or training without a risk-focused plan misses the evaluation and prioritization; ignoring risk and patching only when required is reactive and leaves gaps; treating risk management as solely paperwork reduces it to bureaucracy instead of ongoing protection.

8. What are some of the events logged by the Master Station Log?

A. Weather events, Transportation logs, Vendor visits, Deployment start

B. Hardware setup/teardown, Network or service interruptions, project work, changeover, and status updates

C. User login times, Power usage, Cable runs, Maintenance windows

D. Security incidents, Equipment purchases, Training schedules, Changeover

The event types tracked in the Master Station Log are those that reflect the station's operational state and changes that affect its ability to operate. Hardware setup and teardown are logged to provide a clear record of when equipment is added or removed, which helps with troubleshooting, inventories, and accountability. Recording network or service interruptions captures incidents that directly impact connectivity and service delivery, ensuring the team can correlate issues with times and durations. Project work entries show tasks that influence the station's workload or capabilities, keeping everyone aligned on what's being done and why. Changeovers document transitions between configurations, systems, or teams, which is crucial for traceability and smooth handoffs. Status updates provide a concise picture of the current condition and readiness, helping all observers understand where things stand at a glance. In short, this set focuses on concrete changes to the hardware, network, and operational posture of the station, along with ongoing work and current status—precisely what the Master Station Log is designed to record. Other items like weather, vendor visits, power usage, or training schedules don't consistently represent the day-to-day operational changes the log is meant to capture, so they aren't as fitting for this purpose.

9. What is the difference between incident response and incident handling in cyberspace operations?

A. Incident response is the overall process of detecting, containing, and recovering from an incident; incident handling is the day-to-day management and coordination.

B. Incident response is the network monitoring tool; incident handling is the firewall.

C. Incident response is only about reporting incidents; incident handling is about containment.

D. They are the same.

Incidents are managed through two related but distinct roles: incident handling provides the ongoing, day-to-day management and coordination to keep the response organized, while incident response is the full lifecycle of reacting to an incident, from discovery to recovery and learning. Think of it this way: incident handling covers who does what, when they're involved, how we communicate, and how we track and coordinate actions across teams during an incident. It's about the practical, routine management that keeps things moving and ensures everyone stays informed and aligned. Incident response, on the other hand, is the complete sequence of technical and strategic actions taken to address the incident itself—detecting it, containing it to prevent further harm, eradicating the threat, restoring operations, and applying lessons learned to prevent recurrence. So the best choice reflects that separation: incident response is the overall lifecycle of handling an incident, while incident handling is the day-to-day management and coordination that supports that lifecycle. The other descriptions don't capture that lifecycle/coordination distinction.

10. Describe the UDM.

A. Oversees security clearances

B. Manages maintenance schedules

C. Coordinates personnel relocations

D. Manages deployment readiness and training aspects for all deployable personnel and/or cargo within their unit

The Unit Deployment Manager is the person who ensures the unit is ready to deploy by managing everything related to deployment readiness and training for all deployable personnel and cargo. They keep the deployable roster up to date, verify that required training, medical readiness, and security clearances are current, and coordinate pre-deployment processing, muster, and documentation. They also ensure that equipment and cargo are prepared, properly documented, and available for deployment, including manifests and any special handling needs. This role works with the Installation Deployment Officer and unit leadership to identify and close gaps so deployments proceed on schedule.

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!