Control and Reporting Center (CRC) Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

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 **16**

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. **Which of the following best describes what 'mean time to detect' measures?**

   A. Time to identify a threat

   B. Time to fully restore from an incident

   C. Time to notify stakeholders

   D. Time to escalate to leadership

2. **What is CRC's primary function related to business continuity?**

   A. Coordinates incident response to minimize downtime and supports continuity plans.

   B. Manages payroll and HR inquiries.

   C. Develops marketing campaigns for data services.

   D. Handles vendor contracts.

3. **Which statement describes RSAS High's data role?**

   A. To store TPS-75 data.

   B. To receive TPS-75 data and radar data from RSAS Low.

   C. To encrypt data.

   D. To manage power distribution.

4. **What is the function of the AN/TSC-179 Ground Multi-band Terminal (GMT)?**

   A. Airborne transceiver.

   B. Fixed ground-based terminal.

   C. Transportable and deployable system with multi-band capabilities for satellite communications.

   D. Underwater comm system.

5. **Which action is described as a common CRC recovery strategy after a cyber incident?**

   A. Quarantine affected systems

   B. System rebuild

   C. Notify customers

   D. Conduct tabletop exercise

6. The CID in the CRC is described as having what level of capability?

- **A. A limited capability to determine combat identification and disseminate timely, accurate, and relevant positive identification information**
- **B. A comprehensive automated CID capability**
- **C. No CID capability**
- **D. CID is the primary sensor fusion tool**

7. Who does the CRC coordinate with for effective air defense?

- **A. The National Weather Service meteorologist on duty.**
- **B. The United States Army Air Defense Artillery Fire Control Officer and/or Assistant (ADAFCO and/or ADAFCA).**
- **C. The civilian air traffic controller union representative.**
- **D. The base security officer.**

8. In CRC investigations, what do indicators of compromise (IOCs) help with?

- **A. They help detect, attribute, and confirm malicious activity guiding containment and remediation.**
- **B. They store logs for analysis later.**
- **C. They set access control policies.**
- **D. They encrypt data.**

9. How does CRC perform risk assessment during an incident?

- **A. Reassessing budgets for incident response funding.**
- **B. Evaluate threat likelihood and potential impact, prioritize actions, and adjust resource allocation.**
- **C. Decide on staff promotions.**
- **D. Schedule routine maintenance.**

10. What detail is essential in incident ticketing to support resolution?

- **A. Personal opinions**
- **B. Only high-level summary**
- **C. Evidence and timelines**
- **D. Irrelevant logs**

Answers

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

Explanations

1. Which of the following best describes what 'mean time to detect' measures?

A. Time to identify a threat

B. Time to fully restore from an incident

C. Time to notify stakeholders

D. Time to escalate to leadership

Mean time to detect measures how long it takes, on average, to identify a threat after it begins. It captures detection speed—how quickly monitoring and analysts notice that something is wrong. It's not about restoring services, notifying stakeholders, or escalating to leadership. Those stages fall under other metrics. If a breach starts at a certain time and is detected later, that interval is averaged across incidents to yield the mean time to detect, with lower values indicating faster discovery.

2. What is CRC's primary function related to business continuity?

A. Coordinates incident response to minimize downtime and supports continuity plans.

B. Manages payroll and HR inquiries.

C. Develops marketing campaigns for data services.

D. Handles vendor contracts.

In business continuity, the focus is on how an organization detects, responds to, and recovers from disruptions. The CRC's primary function is to coordinate incident response to minimize downtime and support continuity plans. It serves as the central hub during an incident, bringing together the right people, information, and actions to control the situation, communicate status, and drive recovery steps in line with predefined continuity strategies. This ensures critical services stay available and recovery is aimed at restoring normal operations as quickly as possible. Other activities like payroll and HR inquiries, marketing campaigns for data services, or handling vendor contracts are separate support functions that don't address incident response or continuity planning.

3. Which statement describes RSAS High's data role?

A. To store TPS-75 data.

B. To receive TPS-75 data and radar data from RSAS Low.

C. To encrypt data.

D. To manage power distribution.

In this setup, the important idea is how data moves between RSAS units: RSAS High acts as the higher-level data hub that receives streams from RSAS Low. It gathers inputs from the lower unit to enable centralized processing and fusion at the top level. That's why the statement that RSAS High receives TPS-75 data and radar data from RSAS Low is the best description. It accurately reflects the data flow direction and the role of RSAS High as the collector/processor of incoming sensor information. The other descriptions describe functions not about data reception from the lower unit—for example, storing data, encrypting data, or managing power distribution. These are separate roles and don't define RSAS High's primary data path in this architecture.

4. What is the function of the AN/TSC-179 Ground Multi-band Terminal (GMT)?

A. Airborne transceiver.

B. Fixed ground-based terminal.

C. Transportable and deployable system with multi-band capabilities for satellite communications.

D. Underwater comm system.

The main idea is that this terminal is a portable, field-ready satellite communications node. It's designed to be moved to a location, quickly set up, and provide multi-band satellite links so a unit can connect to space-based networks without relying on fixed infrastructure. The "Ground Multi-band Terminal" part emphasizes it operates on the ground, and the transportable and deployable nature means it's built for rapid deployment in the field, across different frequency bands to access multiple satellite systems. This enables reliable voice and data links between deployed forces and higher headquarters or other networks, even in challenging environments. It's not an airborne transceiver, not a permanently fixed installation, and not an underwater communications system.

5. Which action is described as a common CRC recovery strategy after a cyber incident?

A. Quarantine affected systems

B. System rebuild

C. Notify customers

D. Conduct tabletop exercise

Recovery after a cyber incident centers on returning operations to a secure, trusted baseline. Rebuilding systems—typically by reimaging or reinstalling from clean, known-good images and restoring data from verified backups—remains a common recovery strategy because it removes any malware, backdoors, or corrupted configurations and gives you a fresh base to apply patches and hardened settings. This reduces the risk of reinfection and ensures you can validate system integrity before bringing services back online. Quarantining affected systems is about containment during the incident, not the final restoration. Notifying customers is communications, and tabletop exercises are about planning and testing responses, not restoring operations. Rebuilding is the most reliable path to securely restore operations.

6. The CID in the CRC is described as having what level of capability?

A. A limited capability to determine combat identification and disseminate timely, accurate, and relevant positive identification information

B. A comprehensive automated CID capability

C. No CID capability

D. CID is the primary sensor fusion tool

Combat identification within the CRC is described as a limited capability to determine CID and disseminate timely, accurate, and relevant positive identification information to the right units. This reflects a best-effort, human-in-the-loop approach: it aims to produce reliable PID data quickly to prevent fratricide and improve interoperability, but it isn't a fully automated CID system. Constraints such as data quality, network latency, and the need for verification mean the CRC cannot provide comprehensive automatic CID. It isn't zero capability, and CID isn't the sole or primary sensor fusion tool in the CRC.

7. Who does the CRC coordinate with for effective air defense?

A. The National Weather Service meteorologist on duty.

B. The United States Army Air Defense Artillery Fire Control Officer and/or Assistant (ADAFCO and/or ADAFCA).

C. The civilian air traffic controller union representative.

D. The base security officer.

Effective air defense relies on seamless weapons control and engagement coordination between your control and reporting center and the people who actually direct fires. The CRC provides the air picture, tracks, and battle management, but translating those tracks into timely interceptions is handled by the Fire Control Officer and the Fire Control Assistant (ADAFCO/ADAFCA). They manage weapons direction, develop engagement solutions, and authorize or coordinate interceptor missiles or fighter responses based on rules of engagement and current threat data. This partnership ensures the right asset is directed at the right target with proper timing and coordination across sensors and shooters. Weather updates, while important for operations, come from meteorology and aren't the primary mechanism for air-defense engagement decisions. A civilian air traffic controller union representative isn't part of the tactical engagement chain, and the base security officer handles base protection rather than directing air-defense fires.

8. In CRC investigations, what do indicators of compromise (IOCs) help with?

A. They help detect, attribute, and confirm malicious activity guiding containment and remediation.

B. They store logs for analysis later.

C. They set access control policies.

D. They encrypt data.

Indicators of compromise are signals that appear on systems or networks—like file hashes, suspicious IPs or domains, registry keys, or unusual process behavior—that point to malicious activity. In CRC investigations, they're used to detect that something bad is happening, attribute the activity to a particular attacker or campaign, and confirm that an incident is underway. This helps guide what you do next: containment decisions (for example, isolating affected machines or blocking known malicious indicators) and remediation actions (such as removing the malware, patching vulnerabilities, resetting credentials). While collecting and reviewing logs is important for analysis, the specific signals provided by IOCs are the actionable pointers that drive detection, attribution, confirmation, and the immediate response steps. The other options focus on data storage, access controls, or encryption, which are separate security functions and not the purpose of IOCs.

9. How does CRC perform risk assessment during an incident?

A. Reassessing budgets for incident response funding.

B. Evaluate threat likelihood and potential impact, prioritize actions, and adjust resource allocation.

C. Decide on staff promotions.

D. Schedule routine maintenance.

During an incident, decisions hinge on risk-based awareness of what could go wrong and how bad it would be if it does. The idea is to rapidly estimate how likely a threat is and what impact it could have on essential operations, and then let that risk picture drive what you do first. By evaluating likelihood and potential impact, you can rank actions by priority and move resources—people, tools, and time—where they'll reduce the highest risks the fastest. As the incident evolves, you continuously update this assessment so actions stay aligned with the current risk landscape. Other activities, like revisiting budgets, making personnel promotions, or scheduling routine maintenance, aren't about directing response to the incident or reallocating resources based on risk. They don't address immediate threats or containment priorities, which is why they don't fit the concept of risk assessment during an incident.

10. What detail is essential in incident ticketing to support resolution?

A. Personal opinions

B. Only high-level summary

C. Evidence and timelines

D. Irrelevant logs

Capturing concrete evidence and a precise timeline is essential in incident ticketing because it creates a verifiable trail of what happened and when, which is what enables accurate diagnosis and effective resolution. Evidence such as error messages, system logs, screenshots, configuration details, and performance metrics helps you reproduce the issue, understand impact, and verify that the fix actually addresses the root cause. A clear timeline records when the incident began, when it was detected, the actions taken, who performed them, and when the incident was resolved. This supports rapid triage, coordination across teams, accountability, and useful post-incident reviews to prevent recurrence. Personal opinions don't provide verifiable guidance, a high-level summary lacks the specifics needed to diagnose and reproduce, and irrelevant logs just add noise and slow things down.

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://controlreportingcenter.examzify.com

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