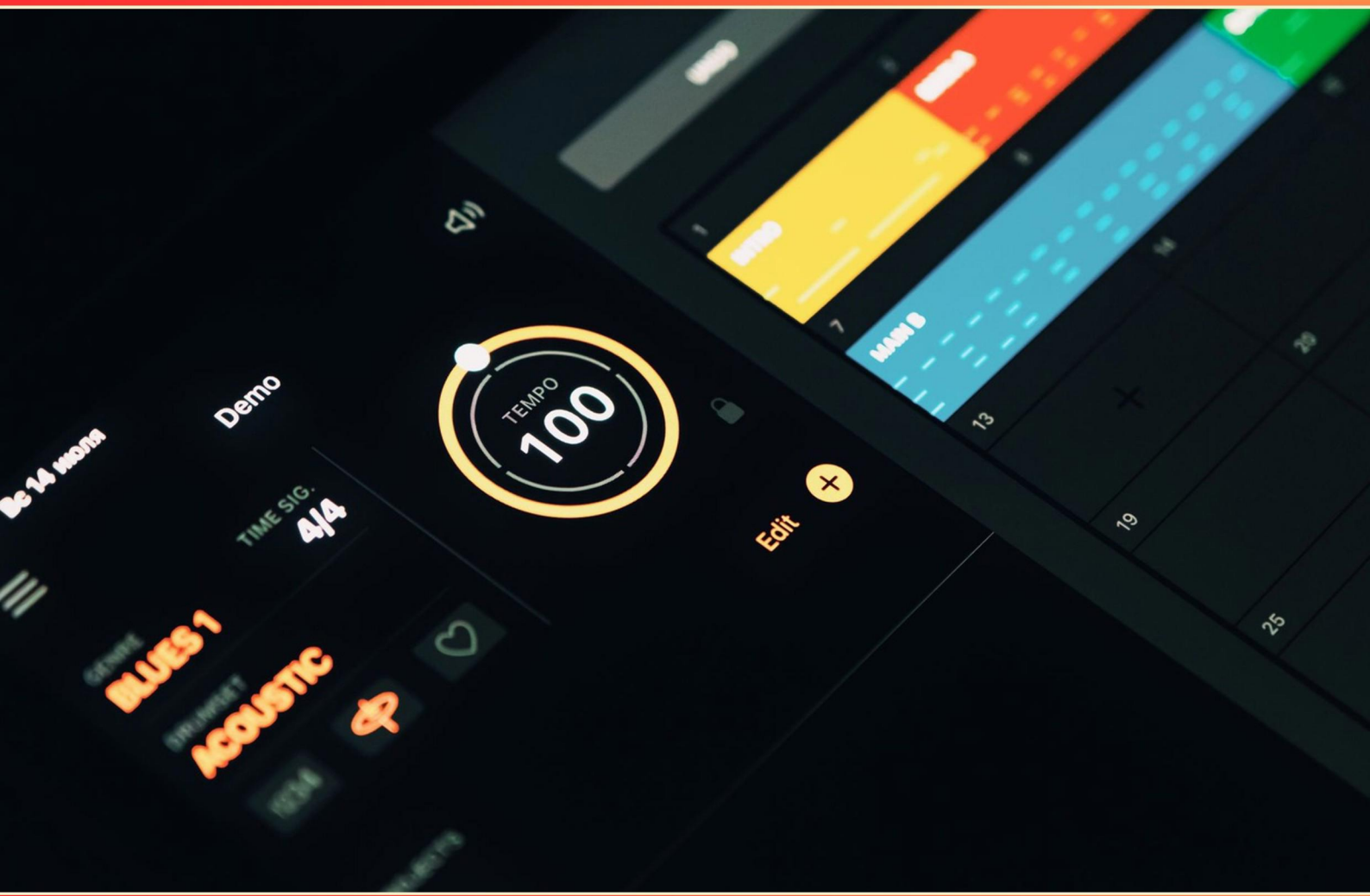
CONTROL AND REPORTING CENTER (CRC) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://controlreportingcenter.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 the term 'situational awareness' refer to in BMC2?

A. The ability to predict weather events

B. The understanding of the operational environment and the status of friendly and enemy forces

C. The discipline of maintaining paper logs

D. The capability to deploy forces without communications

2. What is the role of the Mission Commander (CC)?

A. To oversee the overall mission and ensure effective operations of the Sensor Operations Team.

B. To route data to ADSI.

C. To provide TACSAT DAMA data link.

D. To manage environmental controls.

3. The ADSI Server participates in which type of networks?

A. Tactical data link networks.

B. Voice communication networks only.

C. Weather data networks.

D. Power distribution networks.

4. Which CRC role leads the response during an incident?

A. Incident Controller

B. CRC Manager

C. Liaison Officer

D. Communications Officer

5. Which roles are included among the main components of the Sensor Operations Team (SOT)?

A. AST/SSO, ICT, EPT, and ST/MSO

B. ABM, BMT, WD, ADAFCO

C. ADAFCO, ADAFCA, SOT, ABM

D. MWD, MSO, CC, ICT

6. What are the four severity levels commonly used to classify CRC incidents?

A. High, Medium, Low, Critical

B. Severe, Major, Medium, Low

C. Critical, High, Medium, Low

D. Critical, High, Medium, Informational

7. How does CRC ensure data privacy during incident reporting?

A. Publishing all data publicly

B. Redacting or anonymizing personal data, limiting access, and complying with privacy laws and regulations

C. Disregarding access controls

D. Allowing unrestricted data sharing with third parties

8. What is the purpose of log management in CRC operations?

A. To collect, store, search, and analyze logs for detecting incidents and reconstructing events.

B. To encrypt logs and delete after 24 hours.

C. To preserve logs only for regulatory audits.

D. To share raw logs publicly.

9. What are the main components of the Sensor Operations Team (SOT)?

A. Air Surveillance Technician (AST)/Senior System Operator (SSO), Interface Control Technician(s) (ICT), Electronic Protection Technician(s) (EPT), and Surveillance Technicians (ST)/Mission System Operators (MSO).

B. ABM, BMT, WD, ADAFCO.

C. AST, ICT, WD, ABM.

D. ADAFCO, ADAFCA, ABM, WD.

10. Which teams constitute the CRC mission crew?

A. Battle Management Team (BMT) and Sensor Operations Team (SOT)

B. Air Defense Artillery Fire Control Officer/Assistant (ADAFCO/ADAFCA) only

C. Weapons Director (WD) and Battle Management Team (BMT)

D. Air Surveillance Technician (AST) and Interface Control Technician (ICT)

Answers

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

Explanations

1. What does the term 'situational awareness' refer to in BMC2?

A. The ability to predict weather events

B. The understanding of the operational environment and the status of friendly and enemy forces

C. The discipline of maintaining paper logs

D. The capability to deploy forces without communications

Situational awareness in BMC2 means having a clear, accurate picture of the operating environment and the status of both friendly and enemy forces. It combines data from sensors, reports, and command-and-control systems to show where forces are, what assets are available, and what threats or opportunities exist. This shared understanding lets commanders anticipate changes, coordinate actions, and make timely, informed decisions to keep operations safe and effective. While weather information is useful for planning, it isn't what defines situational awareness in this context; maintaining paper logs is an administrative task, and deploying without communications would degrade the ability to maintain awareness rather than define it.

2. What is the role of the Mission Commander (CC)?

A. To oversee the overall mission and ensure effective operations of the Sensor Operations Team.

B. To route data to ADSI.

C. To provide TACSAT DAMA data link.

D. To manage environmental controls.

The Mission Commander is the overall leader of the operation, responsible for directing the mission and ensuring the Sensor Operations Team functions effectively. This role involves planning and coordinating activities, maintaining a clear picture of the mission's status, allocating resources, monitoring progress and safety, and communicating with higher command to keep everyone informed and aligned. The other tasks listed—routing data to ADSI, providing the TACSAT data link, or managing environmental controls—are specialized technical or support duties carried out by other crew members or sections, not by the Mission Commander.

3. The ADSI Server participates in which type of networks?

A. Tactical data link networks.

B. Voice communication networks only.

C. Weather data networks.

D. Power distribution networks.

The ADSI Server is designed to operate within tactical data link networks, where real-time digital information is shared among military platforms. These networks connect aircraft, ships, and ground units to exchange track data, positions, statuses, and other tactical information to create a common operating picture. That data-sharing role aligns with what the ADSI Server does, making it a participant in tactical data link networks. It isn't meant for voice-only networks, which don't handle the same data payloads, nor for weather data networks or power distribution networks, which serve different purposes and data types.

4. Which CRC role leads the response during an incident?

A. Incident Controller

B. CRC Manager

C. Liaison Officer

D. Communications Officer

Leading the response is about command and control on the scene. The Incident Controller is the person with the authority to direct all actions, set incident objectives, prioritize tasks, allocate resources, and ensure the safety and welfare of responders. This role maintains overall situational awareness and makes the strategic decisions that shape how the response unfolds. The CRC Manager provides broader support to the CRC functions and resources, but does not take on the on-scene leadership role. The Liaison Officer focuses on coordinating with external agencies and stakeholders, ensuring information flows between groups. The Communications Officer handles messaging and information management, keeping people informed but not directing incident tactics.

5. Which roles are included among the main components of the Sensor Operations Team (SOT)?

A. AST/SSO, ICT, EPT, and ST/MSO

B. ABM, BMT, WD, ADAFCO

C. ADAFCO, ADAFCA, SOT, ABM

D. MWD, MSO, CC, ICT

Sensor operations rely on four core roles that cover the essential functions: operating and monitoring the sensors, providing the information and communications technology support, handling the processing and exploitation of sensor data, and supervising the team. The four roles listed—AST/SSO, ICT, EPT, and ST/MSO—together map to those functions, giving a complete SOT makeup. AST/SSO handles the day-to-day sensor operation and surveillance tasks, ICT ensures the data and systems stay connected and integrated, EPT takes the sensor outputs and converts them into usable information, and ST/MSO provides leadership and coordination for the team. This combination ensures sensors are run effectively, data flows smoothly, information is derived efficiently, and the team stays organized. Other options include roles that are not designated as part of the main Sensor Operations Team components or omit one of these essential functions, so they don't form the full SOT set.

6. What are the four severity levels commonly used to classify CRC incidents?

A. High, Medium, Low, Critical

B. Severe, Major, Medium, Low

C. Critical, High, Medium, Low

D. Critical, High, Medium, Informational

The idea behind incident severity is to rank impact so you can decide how urgently to respond. The four levels used in CRC incident classification are Critical, High, Medium, Low, listed from the highest to the lowest impact. Critical means the incident causes the most significant disruption—think widespread service outage, major data exposure, or regulatory risk that affects business operations and requires immediate, high-priority action. High follows for serious impact that's disruptive but not at the level of a full-scale crisis. Medium covers moderate impact that's noticeable and needs standard handling, while Low is for minor issues with little or no operational effect. Other option choices include terms like Informational or Nonstandard levels, which aren't part of the typical CRC severity scale, or they present a different set of terms. The four-term spectrum above—Critical, High, Medium, Low—is the standard framework used to guide escalation and response priorities.

7. How does CRC ensure data privacy during incident reporting?

A. Publishing all data publicly

B. Redacting or anonymizing personal data, limiting access, and complying with privacy laws and regulations

C. Disregarding access controls

D. Allowing unrestricted data sharing with third parties

Protecting personal information is key when incident reports are created and shared. The best approach is to redact or anonymize any personal data so individuals can't be identified, use identifiers that don't reveal who is involved, and apply the principle of data minimization. Limiting access to the reports to only those who need to see them reduces the risk of accidental disclosure or misuse. And proceeding in line with privacy laws and regulations ensures the processing of data has a lawful basis, appropriate safeguards, and rights for data subjects are respected. Publishing everything publicly would expose individuals and violate privacy expectations and laws. Not enforcing access controls or sharing data without restrictions would similarly risk inappropriate exposure and noncompliance. So the combination of redaction/anonymization, restricted access, and regulatory compliance best safeguards privacy during incident reporting.

8. What is the purpose of log management in CRC operations?

A. To collect, store, search, and analyze logs for detecting incidents and reconstructing events.

B. To encrypt logs and delete after 24 hours.

C. To preserve logs only for regulatory audits.

D. To share raw logs publicly.

Gathering and organizing log data across the environment gives you visibility to what happened and when. By collecting, storing, searching, and analyzing logs from systems, networks, and applications, you create a central record of activity that can be examined to detect incidents and piece together the sequence of events. This centralized log view lets you correlate different events—such as authentication attempts, access to sensitive assets, and security alerts—so you can spot unusual patterns, trigger alerts in real time, and build a timeline for investigations. The ability to search and analyze logs supports both immediate response and thorough post-incident forensic work, helping you understand root causes, containment steps, and remediation. Retention and protection of logs are important, but encryption with rapid deletion would undermine the ability to investigate and reconstruct events, while preserving logs only for audits or sharing them publicly would miss the core goal of maintaining situational awareness and actionable insight.

9. What are the main components of the Sensor Operations Team (SOT)?

A. Air Surveillance Technician (AST)/Senior System Operator (SSO), Interface Control Technician(s) (ICT), Electronic Protection Technician(s) (EPT), and Surveillance Technicians (ST)/Mission System Operators (MSO).

B. ABM, BMT, WD, ADAFCO.

C. AST, ICT, WD, ABM.

D. ADAFCO, ADAFCA, ABM, WD.

The main concept being tested is who actually operates and maintains the sensor systems that feed surveillance data. The Sensor Operations Team is made up of the roles that directly handle sensors and the data they produce: Air Surveillance Technician and Senior System Operator oversee the sensor operations on the network; Interface Control Technician(s) ensure the data from those sensors is correctly integrated with other systems; Electronic Protection Technician(s) defend the sensor systems from electronic threats and interference; and Surveillance Technician (or Mission System Operator) who run the surveillance gear and manage the data flowing into the mission systems. Together, these roles keep the sensors up, data accurate, and the information usable for the team's missions. Other groupings mix in roles that belong to different functions, such as Air Battle Manager or Battle Management Team, weather-related personnel, or air defense coordination roles. Those are not part of the Sensor Operations Team, so they don't fit as the main components of SOT.

10. Which teams constitute the CRC mission crew?

A. Battle Management Team (BMT) and Sensor Operations Team (SOT)

B. Air Defense Artillery Fire Control Officer/Assistant (ADAFCO/ADAFCA) only

C. Weapons Director (WD) and Battle Management Team (BMT)

D. Air Surveillance Technician (AST) and Interface Control Technician (ICT)

The CRC mission crew is built around two integrated teams: the Battle Management Team and the Sensor Operations Team. The Battle Management Team handles command and control, decision-making, and the allocation of air assets—essentially directing the overall response and coordinating with higher authorities. The Sensor Operations Team runs the sensors, maintains the air picture, tracks targets, and provides the fused sensor data that the Battle Management Team uses to make decisions. The Weapons Director is typically a lead within the Battle Management Team, while the Sensor Operations Team includes specialists like Air Surveillance Technicians and Interface Control Technicians; but you need both teams to have a complete CRC mission crew. Options that focus on only one function or mix roles from different teams don't capture the full crew composition. That's why the correct pairing is Battle Management Team and Sensor Operations Team.

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!