

British Columbia Security Guard License - BST Exam & Practice Test (2026) (Sample)

Study Guide



Everything you need from our exam experts!

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	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 is a risk management strategy for a security officer?**
 - A. Ignoring minor threats**
 - B. Identifying potential threats**
 - C. Delaying response actions**
 - D. Making assumptions about situations**
- 2. In what situation should a security officer call for law enforcement?**
 - A. Whenever an incident occurs**
 - B. When they feel unsafe or witness a crime**
 - C. Only if requested by a supervisor**
 - D. At the end of their shift if nothing else is resolved**
- 3. How should security personnel manage sensitive information?**
 - A. Share it with all employees**
 - B. Protect it diligently and only share it with authorized individuals**
 - C. Store it on personal devices**
 - D. Leave it unsecured if not in use**
- 4. What is a common reporting tool used by security personnel?**
 - A. Incident Report Form**
 - B. Daily Activity Report (DAR)**
 - C. Security Evaluation Sheet**
 - D. Visitor Log**
- 5. What is the minimum age requirement to work in a security position in British Columbia?**
 - A. 18 years old**
 - B. 19 years old**
 - C. 21 years old**
 - D. 16 years old**

- 6. What is the first action a security officer should take after a security incident?**
 - A. Move the area to avoid further incidents**
 - B. Report the incident to the supervisor and document everything**
 - C. Discuss the incident with bystanders**
 - D. Call law enforcement immediately**
- 7. What is the correct response if a security guard observes a criminal act in progress?**
 - A. Attempt to apprehend the suspect**
 - B. Notify law enforcement and document the incident**
 - C. Ignore it unless it escalates**
 - D. Notify a supervisor only**
- 8. When is it appropriate for a security guard to use physical restraint?**
 - A. Only in emergencies, with no other options available**
 - B. Whenever they feel threatened**
 - C. Only if absolutely necessary to prevent imminent harm to themselves or others**
 - D. When instructed by a supervisor**
- 9. In a fire emergency, what should a security officer prioritize?**
 - A. Evacuating individuals to safety and calling emergency services**
 - B. Collecting all valuables from the area**
 - C. Documenting the incident for future reference**
 - D. Providing first aid to injured individuals**
- 10. What is a common misconception about the security industry?**
 - A. That security personnel can arrest individuals**
 - B. That security personnel have the same authority and training as police officers**
 - C. That all security officers are former military personnel**
 - D. That security personnel work alone without any support**

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which of the following is a risk management strategy for a security officer?

- A. Ignoring minor threats**
- B. Identifying potential threats**
- C. Delaying response actions**
- D. Making assumptions about situations**

Identifying potential threats is a fundamental risk management strategy for a security officer. This proactive approach allows security personnel to assess and understand the environment they are operating in. By recognizing potential risks—whether they are physical, procedural, or personnel-related—security officers can take appropriate measures to mitigate these threats before they escalate into actual incidents. This could involve implementing preventative measures, developing response plans, or increasing surveillance in certain areas. Effective threat identification enables security officers to prioritize their actions based on the likelihood and potential impact of various risks. This strategy is essential not only for protecting property and personnel but also for maintaining a safe environment. In contrast, falling into the other behaviors, such as ignoring threats or making assumptions, would hinder the effectiveness of risk management and could expose individuals and assets to unnecessary dangers.

2. In what situation should a security officer call for law enforcement?

- A. Whenever an incident occurs**
- B. When they feel unsafe or witness a crime**
- C. Only if requested by a supervisor**
- D. At the end of their shift if nothing else is resolved**

A security officer should call for law enforcement when they feel unsafe or witness a crime because their primary responsibility includes ensuring the safety and security of people and property. In situations where an officer observes illegal activity, a potential threat to individuals, or personal danger, immediate law enforcement involvement can be crucial. This ensures that the situation is handled by trained professionals who are equipped to manage criminal behavior and restore order. Having the judgement to call for help not only enhances the response to the incident but also provides necessary support to the security personnel and affected individuals. This proactive approach helps prevent escalation of the situation and ensures that appropriate legal procedures are followed. The other options do not emphasize the critical judgment and situational awareness required in security roles. For instance, calling for law enforcement whenever an incident occurs may lead to unnecessary involvement in trivial matters, while waiting for a supervisor's request could delay critical response actions. Additionally, waiting until the end of a shift could leave potential escalations unchecked, which goes against the security officer's duty to maintain safety at all times.

3. How should security personnel manage sensitive information?

- A. Share it with all employees
- B. Protect it diligently and only share it with authorized individuals**
- C. Store it on personal devices
- D. Leave it unsecured if not in use

Managing sensitive information is critical in security operations. The correct approach is to protect sensitive information diligently and to share it only with individuals who have the proper authorization. This ensures that confidential data remains secure from unauthorized access or disclosure, which can lead to potential risks such as data breaches or compromised security systems. By safeguarding sensitive information, security personnel help maintain the trust of those involved, whether it be employees, clients, or stakeholders. Compliance with applicable laws and regulations is also a key factor, as mishandling sensitive information can lead to legal repercussions for both individuals and organizations. The other options represent practices that can jeopardize the integrity and confidentiality of sensitive information. Sharing it with all employees dilutes the control over who has access to that information, leading to potential misuse. Storing sensitive data on personal devices increases the risk of it being lost or compromised, as personal devices may not have the same security measures in place as company systems. Leaving sensitive information unsecured when not in use is inherently risky as it opens the door for unauthorized access. Therefore, careful management and controlled sharing of information are essential responsibilities of security personnel.

4. What is a common reporting tool used by security personnel?

- A. Incident Report Form
- B. Daily Activity Report (DAR)**
- C. Security Evaluation Sheet
- D. Visitor Log

The Daily Activity Report (DAR) serves as a vital reporting tool for security personnel, as it facilitates continuous documentation of daily activities and observations. This report provides a comprehensive overview of the events that occurred during a specific shift or period, enabling security staff to keep track of security-related incidents, routine inspections, and any noteworthy occurrences. The DAR is crucial for maintaining accurate records, which can later be referenced if an issue arises or if a more detailed report is necessary. It helps in ensuring accountability and transparency within the security team and serves as a resource for evaluation and reporting to supervisors or management. While the Incident Report Form is significant for documenting specific incidents, the DAR captures a broader scope of day-to-day activities, making it a commonly used tool in the field. The other potential responses, such as the Security Evaluation Sheet and Visitor Log, serve more specialized purposes but do not encompass the comprehensive daily overview that the DAR provides.

5. What is the minimum age requirement to work in a security position in British Columbia?

- A. 18 years old**
- B. 19 years old**
- C. 21 years old**
- D. 16 years old**

The minimum age requirement to work in a security position in British Columbia is 19 years old. This regulation is in place because security roles often involve responsibilities that require a certain level of maturity and judgment, such as dealing with potentially volatile situations or making quick decisions that impact public safety. By establishing 19 as the minimum age, the province ensures that individuals in these positions are legally recognized as adults in British Columbia, capable of handling the complexities and responsibilities associated with security work. This age requirement reflects not just a legal standard but also acknowledges the importance of experience and maturity in effectively performing security duties. As individuals in this field are often required to interact with the public, enforce laws, and respond to emergencies, being of legal age ensures that they have the capability to fulfill these duties thoughtfully and responsibly.

6. What is the first action a security officer should take after a security incident?

- A. Move the area to avoid further incidents**
- B. Report the incident to the supervisor and document everything**
- C. Discuss the incident with bystanders**
- D. Call law enforcement immediately**

After a security incident, the first action a security officer should take is to report the incident to the supervisor and document everything. This step is crucial because it ensures that the details of the incident are properly recorded while the information is still fresh in the minds of those involved. Accurate documentation is key for any subsequent investigations, claims, or reviews of the incident, as it provides a clear account of what occurred, who was involved, and any actions taken in response. Reporting to a supervisor places the incident within the chain of command, allowing for appropriate responses and further actions to be taken at a higher level. Additionally, having a complete and thorough documentation process can protect the security officer and the organization by providing a record that can be referred to in the future, whether for legal reasons or for improving security protocols. In contrast to other options, immediately discussing the incident with bystanders might lead to misinformation or confusion, and moving the area to avoid further incidents should only be done if it is safe and necessary, rather than as a first priority. Calling law enforcement is also important but typically occurs after reporting internally, depending on the severity of the incident.

7. What is the correct response if a security guard observes a criminal act in progress?

- A. Attempt to apprehend the suspect**
- B. Notify law enforcement and document the incident**
- C. Ignore it unless it escalates**
- D. Notify a supervisor only**

The appropriate response when a security guard observes a criminal act in progress is to notify law enforcement and document the incident. This approach is critical for several reasons. First, security personnel are not law enforcement officers, and attempting to apprehend a suspect can put them in danger, as they may lack the training, authority, or resources that law enforcement possesses. Ensuring safety is paramount, not only for the guard but also for bystanders and the suspects involved. Second, promptly informing law enforcement ensures that trained professionals are on the scene to handle the situation according to legal and procedural standards. They have the expertise to manage potentially volatile situations without escalation. Documenting the incident is equally important as it provides an official record of what transpired. This documentation can be crucial for investigations, potential court cases, or insurance claims. Accurate reporting helps law enforcement understand the context and details of the crime better. In summary, notifying law enforcement and documenting the incident ensures safety, compliance with legal protocols, and provides a necessary record that can assist in addressing the criminal activity effectively.

8. When is it appropriate for a security guard to use physical restraint?

- A. Only in emergencies, with no other options available**
- B. Whenever they feel threatened**
- C. Only if absolutely necessary to prevent imminent harm to themselves or others**
- D. When instructed by a supervisor**

Using physical restraint as a security guard is a serious matter and is governed by specific guidelines to ensure the safety and well-being of all parties involved. The correct answer addresses the fundamental principle that physical restraint should only be applied when it is absolutely necessary to prevent imminent harm to the security guard, others, or both. This reflects a defensive approach, prioritizing de-escalation and the use of verbal commands before resorting to physical measures. In scenarios where a security guard perceives an immediate threat - for instance, if someone is about to engage in violent behavior or poses a risk to themselves or others - applying physical restraint can be justified to mitigate that specific danger. Security protocols emphasize the necessity of assessing each situation critically and prioritizing non-violent solutions when possible. By restricting the use of physical restraint to situations where harm is imminent, it ensures that security staff act within legal and ethical boundaries, thereby protecting their interests as well as those of others involved. This principle is supported by training that encourages guards to use their judgment and choose less forceful interventions wherever feasible. Options regarding feeling threatened or following a supervisor's instructions without context may lead to inappropriate use of restraint and potentially escalate situations unnecessarily. Therefore, understanding the correct context for physical restraint is crucial for maintaining

9. In a fire emergency, what should a security officer prioritize?

- A. Evacuating individuals to safety and calling emergency services**
- B. Collecting all valuables from the area**
- C. Documenting the incident for future reference**
- D. Providing first aid to injured individuals**

Prioritizing the evacuation of individuals to safety and calling emergency services during a fire emergency is critical for several reasons. First and foremost, the primary goal in such situations is to protect human life. Evacuating individuals ensures that they are moved away from immediate danger and potential injuries caused by fire or smoke inhalation. Calling emergency services is equally vital, as professional firefighters and first responders have the training, equipment, and resources necessary to handle fires effectively. They can manage the situation safely and assist those who may be unable to evacuate on their own. While addressing any injured individuals is important, the immediate focus should be on getting everyone to safety before providing first aid. Collecting valuables could compromise safety and shouldn't take precedence in an emergency. Documenting the incident may be necessary later, but it is not the immediate concern when lives are at stake. The emphasis on prompt evacuation and alerting authorities ensures that the priority is the safety and well-being of all individuals present during a fire emergency.

10. What is a common misconception about the security industry?

- A. That security personnel can arrest individuals**
- B. That security personnel have the same authority and training as police officers**
- C. That all security officers are former military personnel**
- D. That security personnel work alone without any support**

The belief that security personnel have the same authority and training as police officers is a common misconception within the security industry. In reality, while security personnel are trained to protect property and manage safety risks, they do not possess the same legal authority as law enforcement officers. Police officers are sworn representatives of the law with specific legal powers, such as making arrests and conducting investigations, which security professionals do not have. Security personnel's authority is generally limited to the private property they are hired to protect, and they often operate under a different regulatory framework than police. Understanding this distinction clarifies the role of security in relation to law enforcement and helps define the appropriate expectations of their duties.

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://britishcolumbiabasicsecuritytraining.examzify.com>

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