

TSA CYBERSECURITY PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR
THE FULL VERSION STUDY GUIDE

<https://tsacybersecurity.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	16

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.

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

SAMPLE

- 1. Which regulatory body oversees the cybersecurity measures of the TSA?**
 - A. Federal Bureau of Investigation (FBI)
 - B. National Security Agency (NSA)
 - C. Department of Homeland Security (DHS)
 - D. Federal Aviation Administration (FAA)

- 2. What is the term for software that is exclusively controlled by a company and cannot be used or modified without permission?**
 - A. Open-Source Software
 - B. Freeware
 - C. Proprietary Software
 - D. Shareware

- 3. Which of the following is considered personal information?**
 - A. Trade secrets of a company
 - B. Government classified documents
 - C. Social Security numbers
 - D. Company financial reports

- 4. What is the primary responsibility of a Chief Information Security Officer (CISO)?**
 - A. To manage computer hardware
 - B. To oversee the organization's security strategy and program
 - C. To handle customer service issues
 - D. To design software applications

- 5. Which application delivery method should you choose if you want to use an application and are not connected to a network?**
 - A. Cloud Installation
 - B. Local Installation
 - C. Remote Access
 - D. Virtual Machine

- 6. What is the approximate maximum downtime for a system with "five nines" availability?**
- A. 2.63 minutes per year
 - B. 5.26 minutes per year
 - C. 10.5 minutes per year
 - D. 1 hour per year
- 7. What is the primary function of antivirus software?**
- A. To speed up computer performance
 - B. To detect and remove malicious software from a computer system
 - C. To manage network security
 - D. To create backups of data
- 8. You need the most secure method for your wireless network. Which should you implement?**
- A. WPA2
 - B. WEP
 - C. WPA
 - D. Open Network
- 9. Which scenario illustrates the concept of an Access Control List (ACL)?**
- A. A user logs in without restrictions
 - B. A user is restricted from a resource despite being authenticated
 - C. A user can download any files
 - D. A user has access to any network
- 10. Which of the following is NOT a method of data transmission?**
- A. Wired networks
 - B. Wireless networks
 - C. Sneakernet
 - D. Cloud storage

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which regulatory body oversees the cybersecurity measures of the TSA?

- A. Federal Bureau of Investigation (FBI)
- B. National Security Agency (NSA)
- C. Department of Homeland Security (DHS)**
- D. Federal Aviation Administration (FAA)

The correct answer is the Department of Homeland Security (DHS) because it is the primary federal body responsible for protecting the nation's critical infrastructure, including transportation systems. The TSA, or Transportation Security Administration, is an agency within the DHS, which means the DHS oversees its cybersecurity measures as part of a broader mandate to secure transportation and ensure public safety. The role of the DHS includes developing national policies and coordinating efforts across different sectors to enhance cybersecurity effectiveness. Within the transportation domain, the DHS ensures that the TSA implements strategies and practices that mitigate risks associated with cyber threats. While other organizations like the FBI and NSA play critical roles in national security and intelligence, their focus areas differ; the FBI deals with criminal justice and federal law enforcement, and the NSA primarily works on signals intelligence and information assurance. The FAA is responsible for civil aviation safety, but it does not have jurisdiction over cybersecurity measures specifically related to the TSA. Thus, the oversight of TSA's cybersecurity measures falls squarely under the responsibilities of the DHS.

2. What is the term for software that is exclusively controlled by a company and cannot be used or modified without permission?

- A. Open-Source Software
- B. Freeware
- C. Proprietary Software**
- D. Shareware

Proprietary software refers to programs that are owned by an individual or a company, granting that entity full control over its use, distribution, and modification. This means that users need permission to access the source code, make alterations, or redistribute the software. Proprietary software typically comes with a license that outlines how it can be used, which often requires payment or subscription to maintain legal access. In contrast, open-source software allows users to view, modify, and distribute the source code, fostering collaboration and innovation. Freeware is software that is available for use at no monetary cost but may still have restrictions regarding modification or redistribution. Shareware is a type of software that is distributed on a trial basis and often requires payment for continued use, but may allow users to explore functionalities before purchasing. Understanding these distinctions is crucial for navigating software licensing and development, especially in environments that prioritize security and compliance.

3. Which of the following is considered personal information?

- A. Trade secrets of a company
- B. Government classified documents
- C. Social Security numbers**
- D. Company financial reports

The correct answer is identified as Social Security numbers, as these are explicitly classified as personal information. Personal information typically refers to data that can be used to identify an individual or involves sensitive details about an individual. Social Security numbers (SSNs) are unique identifiers used primarily in the United States to track individuals for taxation and benefits purposes. The unauthorized disclosure of SSNs can lead to identity theft and other significant privacy violations. In contrast, trade secrets of a company, government classified documents, and company financial reports do not fall under the category of personal information. Trade secrets are proprietary business information that provides a company with a competitive edge and are not linked to personal identities. Government classified documents pertain to national security and are intended for official use only, lacking direct relevance to personal information. Similarly, company financial reports primarily concern corporate details and performance metrics and don't contain identifiable personal data about individuals.

4. What is the primary responsibility of a Chief Information Security Officer (CISO)?

- A. To manage computer hardware
- B. To oversee the organization's security strategy and program**
- C. To handle customer service issues
- D. To design software applications

The primary responsibility of a Chief Information Security Officer (CISO) is to oversee the organization's security strategy and program. This role is critical in ensuring that the organization's information assets are adequately protected against cybersecurity threats. The CISO develops and implements security policies, manages security initiatives, and responds to incidents affecting the organization's information systems. By establishing a comprehensive security framework, the CISO ensures compliance with relevant laws and regulations while aligning security goals with the organization's overall objectives. Unlike the responsibilities related to managing computer hardware, handling customer service issues, or designing software applications, the role of a CISO is centered specifically on the protection of the organization's data and its information technology environment. This focus on security strategy encompasses risk management, incident response, and ongoing evaluation of the security posture, which are crucial for maintaining the integrity and confidentiality of sensitive information.

5. Which application delivery method should you choose if you want to use an application and are not connected to a network?

- A. Cloud Installation
- B. Local Installation**
- C. Remote Access
- D. Virtual Machine

Choosing local installation as the application delivery method is appropriate when you want to use an application without being connected to a network. A local installation involves downloading the application's files onto your device's hard drive, allowing you to run it independently of any internet connection. This method ensures that you have direct access to the application at all times and can use its full functionality regardless of your connectivity status. In contrast, cloud installation relies on internet access, as applications are hosted on remote servers and must be streamed or downloaded from the cloud each time they are accessed. Remote access involves connecting to an application that runs on another computer or server, which also requires a network connection. Virtual machines simulate an entire operating system with applications that might need network connectivity depending on how they are configured. These methods do not allow use of the application without a network, making local installation the best choice for offline access.

6. What is the approximate maximum downtime for a system with "five nines" availability?

- A. 2.63 minutes per year
- B. 5.26 minutes per year**
- C. 10.5 minutes per year
- D. 1 hour per year

The concept of "five nines" availability refers to a system being operational 99.999% of the time. To calculate the maximum allowable downtime in a year, you can start by understanding that one year has 525,600 minutes (60 minutes per hour multiplied by 24 hours a day times 365 days a year). To determine the maximum downtime, you multiply the total minutes in a year by the percentage of downtime allowed for five nines availability. The total downtime can be calculated as follows: 1. Calculate the percentage of downtime: $100\% - 99.999\% = 0.001\%$ downtime. 2. Convert that percentage to minutes: 0.00001 (which is 0.001% as a decimal) multiplied by 525,600 minutes results in approximately 5.26 minutes per year. Therefore, if a system operates at the five nines level of availability, it means that it is extremely reliable, with only about 5.26 minutes of downtime permitted throughout the entire year. This aligns with the understanding of high-availability systems in IT and the standards set for mission-critical applications where uptime is a top priority.

7. What is the primary function of antivirus software?

- A. To speed up computer performance
- B. To detect and remove malicious software from a computer system**
- C. To manage network security
- D. To create backups of data

The primary function of antivirus software is to detect and remove malicious software from a computer system. This includes various types of threats such as viruses, worms, Trojans, ransomware, and spyware that can harm computer systems or compromise sensitive data. Antivirus programs use a combination of techniques to identify malicious software, including signature-based detection, heuristic analysis, and behavior-based detection. Once identified, the software can quarantine or remove the malicious files, helping to ensure that the system remains secure and operational. The other options, while related to common tasks associated with overall computer maintenance and security, do not specifically define the core purpose of antivirus software. For instance, speeding up computer performance is typically managed through optimization tools rather than antivirus functions. Managing network security involves a broader range of technologies and strategies, including firewalls and intrusion detection systems, and creating data backups is a separate function aimed at data redundancy and recovery, not directly linked to the role of antivirus software.

8. You need the most secure method for your wireless network. Which should you implement?

- A. WPA2**
- B. WEP
- C. WPA
- D. Open Network

WPA2 is the most secure method among the options presented for securing a wireless network. It stands for Wi-Fi Protected Access II and implements strong encryption standards, specifically using the Advanced Encryption Standard (AES). This encryption protocol is significantly more secure than its predecessor, WPA, which utilized TKIP (Temporal Key Integrity Protocol) that is more vulnerable to attacks. WPA2 also offers improved authentication methods and better overall security when configured correctly. It is designed to address many of the vulnerabilities that were present in earlier wireless security protocols like WEP (Wired Equivalent Privacy), which is now considered obsolete due to numerous security flaws that allow for relatively easy breaches. An open network, which lacks any encryption, does not provide any security whatsoever, leaving users' data completely exposed to potential eavesdropping and unauthorized access. Choosing WPA2 helps ensure the protection of sensitive information as data is transmitted over the wireless network, making it the optimal choice for maintaining security in a wireless environment.

9. Which scenario illustrates the concept of an Access Control List (ACL)?

- A. A user logs in without restrictions
- B. A user is restricted from a resource despite being authenticated**
- C. A user can download any files
- D. A user has access to any network

The scenario where a user is restricted from a resource despite being authenticated effectively illustrates the concept of an Access Control List (ACL). An ACL is a set of rules that determines which users or systems have permission to access specific resources and what operations they can perform on those resources. In this case, the user is authenticated, meaning they have successfully logged in and their identity has been verified. However, the ACL is enforcing specific permissions that restrict access to certain resources based on defined criteria. This separation between authentication (verifying identity) and authorization (determining what resource access is allowed) is central to effective access control practices in cybersecurity. This scenario emphasizes that access is not solely dependent on the user's identity but rather on the permissions assigned to that identity within the ACL. It highlights the importance of managing who can do what within a system, adhering to the principle of least privilege, which enhances overall security by minimizing potential exposure to sensitive resources.

10. Which of the following is NOT a method of data transmission?

- A. Wired networks
- B. Wireless networks
- C. Sneakernet
- D. Cloud storage**

Data transmission refers to the process of sending and receiving data between devices and systems. The term encompasses various methods used to transfer data, either through physical connections or through wireless means. Wired networks and wireless networks are two primary methods of data transmission. Wired networks utilize physical cables (such as Ethernet cables) for data transfer, while wireless networks use radio waves to transmit data over the air. Sneakernet is a less common method where data is physically transported from one device to another using portable storage media, such as USB drives or external hard drives. Although unconventional, it is still considered a means of data transmission. Cloud storage, on the other hand, refers to a service that allows users to store and access data over the internet through a third-party provider's servers. While cloud storage may facilitate data access and sharing, it does not directly constitute a method of transmitting data itself. Instead, it is a form of data storage and management, where the transmission occurs through the internet, but the primary purpose is to store rather than transmit data.

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://tsacybersecurity.examzify.com>

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

SAMPLE