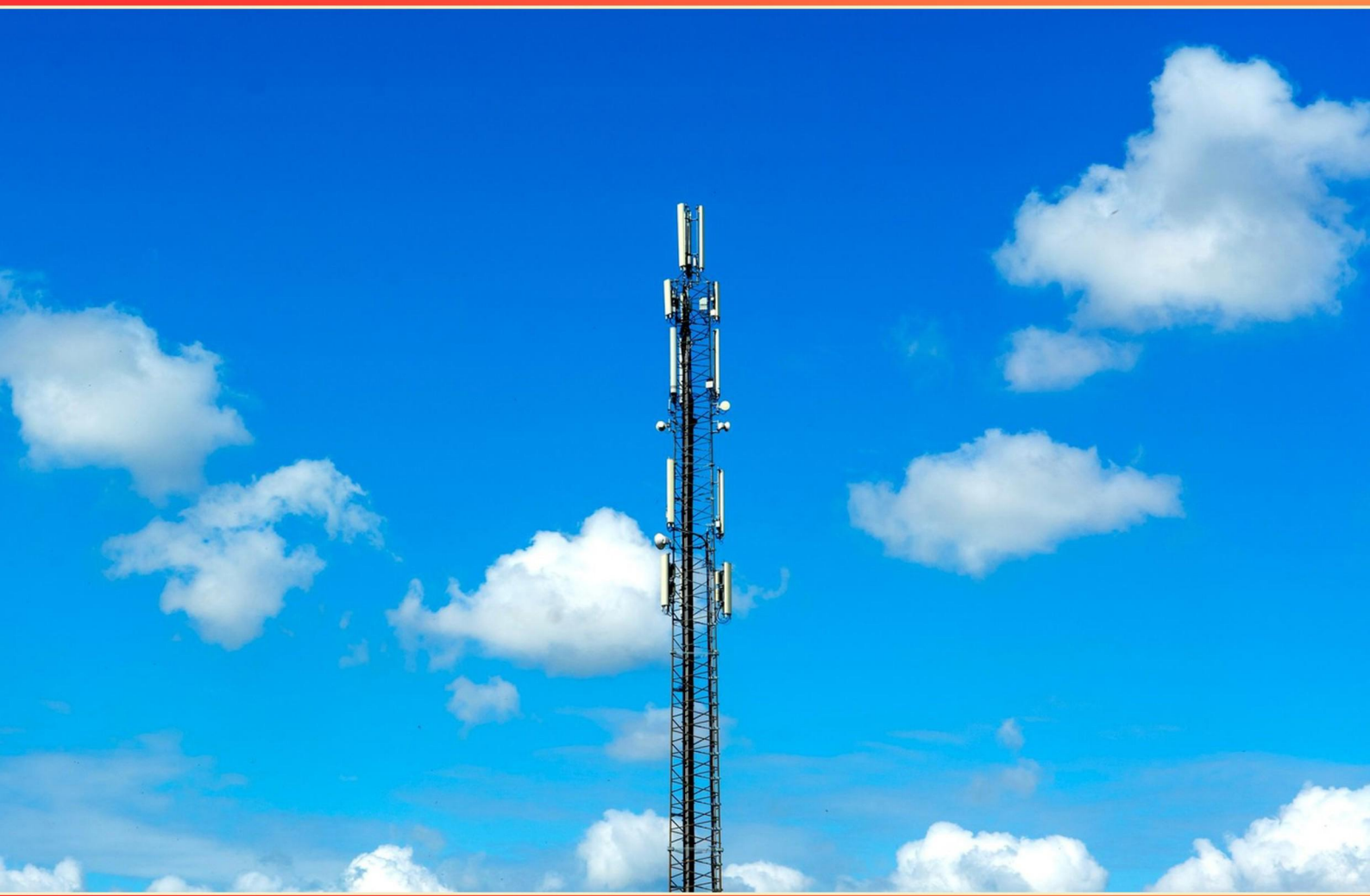
COMPTIA SECURITY+ (SY0-601) CERTIFICATION PRACTICE TEST (SAMPLE)

STUDY GUIDE



Prepare with structure. Pass with confidence

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

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. **Which solution should a security administrator implement to reduce time spent on common security tasks without increasing staff?**

   A. DAC

   B. ABAC

   C. SCAP

   D. SOAR

2. **Which two elements are essential for maintaining optimal environmental temperature in a data center layout?**

   A. An air gap and a hot aisle

   B. A cold aisle and removable doors

   C. An IoT thermostat and a humidity monitor

   D. A hot aisle and a cold aisle

3. **Which method would help identify potential vulnerabilities on hosted web servers running outdated software?**

   A. Hping3 -s comptia, org -p 80

   B. Nc -1 -v comptia, org -p 80

   C. nmp comptia, org -p 80 -aV

   D. nslookup -port=80 comtia.org

4. **What is the primary concern of the company when they clean whiteboards and clear desks before a tour?**

   A. Loss of proprietary information

   B. Damage to the company's reputation

   C. Social engineering

   D. Credential exposure

5. **Which measure is crucial to preventing data breaches in mobile devices?**

   A. Regular OS updates

   B. Implementing strong passwords

   C. Full-device encryption

   D. Limiting app installations

SAMPLE

6. What solution can help ensure availability of point-of-sale systems during peak sales periods?

A. Database backups

B. Network monitoring

C. Load balancing

D. Service patches

7. In the context of risk management, what does RPO stand for?

A. Recovery Point Objective

B. Recovery Planning Options

C. Risk Protection Order

D. Risk Potential Outcome

8. Which application attack is being tested if the URL shows a session ID after clicking a link?

A. Pass-the-hash

B. Session replay

C. Object deference

D. Cross-site request forgery

9. What is the BEST document to establish responsibilities and monetary penalties for managing third-party risk?

A. An ARO

B. An MOU

C. An SLA

D. A BPA

10. When configuring a vulnerability scanner for a global organization, what is the BEST way to mitigate the risk of unauthorized access to service accounts?

A. Create consultant accounts for each region with MFA notifications

B. Create one global administrator account with Kerberos authentication

C. Create different accounts for each region limited by logon times

D. Create guest accounts for each region and block password reuse

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which solution should a security administrator implement to reduce time spent on common security tasks without increasing staff?

A. DAC

B. ABAC

C. SCAP

D. SOAR

The best solution for reducing time spent on common security tasks without increasing staff is SOAR, which stands for Security Orchestration, Automation, and Response. SOAR platforms are designed to automate and orchestrate repetitive security tasks, allowing security teams to work more efficiently. By implementing SOAR, a security administrator can streamline workflows, integrate various security tools, and allow for automatic responses to alerts and incidents, thus minimizing manual workload. This leads to faster incident response times, improved security posture, and more focused personnel who can handle complex tasks rather than repetitive ones. While the other options, such as DAC (Discretionary Access Control), ABAC (Attribute-Based Access Control), and SCAP (Security Content Automation Protocol), have their specific uses in managing security and compliance, they do not inherently focus on automating tasks or orchestrating processes to a degree that SOAR does. Therefore, for the goal of reducing time on common tasks without increasing staff, SOAR is the most appropriate choice.

2. Which two elements are essential for maintaining optimal environmental temperature in a data center layout?

A. An air gap and a hot aisle

B. A cold aisle and removable doors

C. An IoT thermostat and a humidity monitor

D. A hot aisle and a cold aisle

The key to maintaining an optimal environmental temperature in a data center layout primarily involves the strategic arrangement of hot and cold airflows to prevent overheating of equipment. The combination of a hot aisle and a cold aisle is essential in this context. This layout allows for a controlled airflow where cool air is directed toward the front of servers (the cold aisle), while the hot air expelled from the servers is contained in a separate aisle (the hot aisle). In this design, cold aisles contain racks of servers that face each other, allowing the cool air from raised floor vents to be drawn in directly by the servers. The hot aisle, conversely, collects the hot air that is expelled from the backs of the servers, which can then be ventilated out of the data center or redirected appropriately. This organization helps in maximizing cooling efficiency and maintaining equipment performance, thereby significantly reducing the risk of overheating. While using an IoT thermostat and a humidity monitor can enhance monitoring and management, these tools alone do not directly contribute to the structural design necessary for optimal thermal management within the data center, thus making the other arrangement the more foundational element for achieving optimal environmental control.

SAMPLE

3. Which method would help identify potential vulnerabilities on hosted web servers running outdated software?

A. Hping3 -s comptia, org -p 80

B. Nc -1 -v comptia, org -p 80

C. nmp comptia, org -p 80 -aV

D. nslookup -port=80 comtia.org

The method that would effectively help identify potential vulnerabilities on hosted web servers running outdated software is by using the command that employs "nmap" with the service and version detection options. This command scans the target server and attempts to identify the services running on the specified port—in this case, port 80 for HTTP—and it tries to determine their versions. By running an nmap scan with specific flags such as "-sV," which enables version detection, the tool will probe the services running on the server. It identifies the software versions in use, allowing you to assess whether they are outdated or known to have vulnerabilities. This is crucial for security teams as they can then take appropriate actions to patch or mitigate the risks associated with any vulnerable software. In contrast, the other commands listed do not adequately address identifying version information or vulnerabilities in a similar manner. Hping3 is a packet generator and doesn't provide service detection, while Nc (netcat) is primarily for establishing connections and does not analyze service versions. The nslookup command is predominantly used for DNS lookups and does not provide insights into the services or their vulnerabilities on the web server.

4. What is the primary concern of the company when they clean whiteboards and clear desks before a tour?

A. Loss of proprietary information

B. Damage to the company's reputation

C. Social engineering

D. Credential exposure

The primary concern of the company when they clean whiteboards and clear desks before a tour is to mitigate the risks associated with social engineering. Social engineering involves manipulating individuals to gain confidential information or access to their systems and data. By eliminating visible notes, diagrams, or sensitive information that might be left on whiteboards or desks, the company aims to reduce the potential for someone to leverage that information to facilitate social engineering attacks. When visitors tour a facility, they could inadvertently or intentionally observe sensitive information that could be used against the company, leading to security breaches or the exploitation of proprietary information. Therefore, the best practice of cleaning up before a tour directly addresses this concern, ensuring that the company maintains its security posture against such manipulative tactics. Loss of proprietary information, damage to the company's reputation, and credential exposure are valid concerns but are not the primary focus when preparing for a visitor's tour. The emphasis is primarily on safeguarding against information that could be exploited through social interactions rather than direct theft or damage.

SAMPLE

5. Which measure is crucial to preventing data breaches in mobile devices?

A. Regular OS updates

B. Implementing strong passwords

C. Full-device encryption

D. Limiting app installations

Full-device encryption is a crucial measure for preventing data breaches in mobile devices because it helps protect the data stored on the device from unauthorized access. When a device is fully encrypted, the information it contains is transformed into a format that cannot be easily understood without the appropriate decryption keys. This means that if the mobile device is lost, stolen, or accessed by an unauthorized user, the data remains secure and inaccessible without the proper credentials or keys. While other measures such as regular operating system updates, implementing strong passwords, and limiting app installations contribute to overall security, they primarily focus on defense against malware, unauthorized access, and minimizing vulnerabilities rather than directly securing the data itself. With full-device encryption, even if an attacker bypasses other security measures, the data remains protected, making it one of the most effective strategies to safeguard sensitive information on mobile devices.

6. What solution can help ensure availability of point-of-sale systems during peak sales periods?

A. Database backups

B. Network monitoring

C. Load balancing

D. Service patches

Load balancing is the most effective solution for ensuring the availability of point-of-sale systems during peak sales periods. This technique distributes incoming network traffic across multiple servers or resources, which helps to manage and optimize server utilization. By balancing the load, it reduces the risk of any single server becoming overwhelmed during high-traffic times, such as holiday sales or special promotions. This ensures that customers can complete transactions smoothly and effectively, thus maintaining the availability of the point-of-sale system when it is needed most. Database backups, while important for data recovery and integrity, do not directly contribute to system availability during peak times. Network monitoring is essential for maintaining performance and detecting issues but does not inherently prevent overload. Service patches are crucial for security and performance improvements but do not handle the immediate capacity concerns that arise during spikes in transaction volume.

SAMPLE

7. In the context of risk management, what does RPO stand for?

A. Recovery Point Objective

B. Recovery Planning Options

C. Risk Protection Order

D. Risk Potential Outcome

RPO, or Recovery Point Objective, is a critical term in the context of risk management and disaster recovery planning. It defines the maximum age of files that an organization must recover from backup storage for normal operations to resume after a disruption. Essentially, RPO indicates how much data loss is acceptable in terms of time, reflecting the tolerance for potential data loss that could occur if there is a disaster or failure. For example, if an organization's RPO is set at four hours, this means that in the event of a disaster, it must be able to recover data from a backup that is no more than four hours old. This helps organizations establish backup intervals and data protection strategies to ensure that data is effectively safeguarded and can be restored within acceptable limits. The other options presented do not correctly define RPO in risk management terms. Recovery Planning Options may refer to various strategies organizations could employ for recovery, but it does not define a specific metric like the RPO does. Risk Protection Order and Risk Potential Outcome also do not correspond to widely recognized concepts in risk management, further reinforcing that Recovery Point Objective is the accurate term in this context.

8. Which application attack is being tested if the URL shows a session ID after clicking a link?

A. Pass-the-hash

B. Session replay

C. Object deference

D. Cross-site request forgery

The scenario described points to session replay attacks, where an attacker might capture valid session IDs and replay them to access a user's session after the ID has been transmitted over a network. When a URL shows a session ID, it indicates that the application is relying on this identifier to maintain or validate session states. If an attacker can capture this session ID (through methods such as eavesdropping or man-in-the-middle attacks), they can potentially impersonate the legitimate user by reusing the session ID. In the context of application security, revealing session IDs in URLs can expose vulnerabilities because these identifiers can be intercepted or logged in various places (like browser history or server logs). Once the attacker obtains the session ID, they can gain unauthorized access to the user's session. This is why it specifically represents a session replay attack. The other attack types do not relate directly to the exposure of session IDs in the URL. For example, pass-the-hash involves the use of hashed credentials without needing the plaintext password; object deference relates to access control mechanisms being bypassed; and cross-site request forgery (CSRF) involves tricking a user into unknowingly submitting requests to vulnerable applications where they are already authenticated. Hence, each of these paths addresses different

SAMPLE

9. What is the BEST document to establish responsibilities and monetary penalties for managing third-party risk?

A. An ARO

B. An MOU

C. An SLA

D. A BPA

The best document to establish responsibilities and monetary penalties for managing third-party risk is a Memorandum of Understanding (MOU). An MOU serves as a formal agreement between parties that outlines the terms, responsibilities, expectations, and communication points regarding a collaboration or partnership, including how to handle risks associated with third parties. An MOU specifically defines the responsibilities of each party involved and can lay the groundwork for outlining penalties or consequences for failing to fulfill those responsibilities. This makes it an essential document when managing the nuances of third-party risk, ensuring all parties are aware of their commitments and the implications of non-compliance. While other options exist, they do not provide the same level of clarity or specificity for these scenarios. For example, a Service Level Agreement (SLA) focuses largely on the expected level of service and performance output rather than broad risk management and penalties. An Acceptable Risk Outline (ARO) is a framework used for evaluating and communicating risks rather than specifying responsibilities or penalties. A Business Partnership Agreement (BPA) primarily addresses business relationships and financial agreements, rather than explicitly establishing penalties related to third-party risk management.

10. When configuring a vulnerability scanner for a global organization, what is the BEST way to mitigate the risk of unauthorized access to service accounts?

A. Create consultant accounts for each region with MFA notifications

B. Create one global administrator account with Kerberos authentication

C. Create different accounts for each region limited by logon times

D. Create guest accounts for each region and block password reuse

Creating different accounts for each region limited by logon times is the best method to mitigate the risk of unauthorized access to service accounts. This approach allows an organization to establish more granular control over user access and permissions tailored to specific regional requirements. By limiting the accounts to specific logon times, the organization can reduce the window of opportunity for potential attackers to exploit these accounts. Additionally, this method ensures that service accounts are only active during designated times, minimizing the risk of them being compromised outside of operational hours. This practice aligns with the principle of least privilege, allowing users to have only the necessary permissions required for their functions while reducing the risks associated with unauthorized access. The other options suggest different approaches that may not provide the same level of control or flexibility as the chosen option. For example, creating consultant accounts with multifactor authentication might improve security but may be more complex to maintain across regions. A single global administrator account could lead to significant security risks due to the consolidated access it provides. Lastly, guest accounts with blocked password reuse might not be suitable for service accounts needing reliable operational access. Therefore, the chosen answer effectively addresses both security and operational needs.

SAMPLE

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://comptiasecplussy0601.examzify.com

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

SAMPLE