(ISC)2 Certified in Cybersecurity Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

This is a sample study guide. To access the full version with hundreds of questions,

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

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. Don’t worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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 information security strategy integrates people, technology, and operations to establish security barriers?**

    A. Layered Security

    B. Defense in Depth

    C. Multi-Layered Protection

    D. Holistic Security Strategy

2. **Which protocol would help synchronize devices within a company's internal IT environment?**

    A. FTP (File Transfer Protocol)

    B. NTP (Network Time Protocol)

    C. SMTP (Simple Mail Transfer Protocol)

    D. HTTP (Hypertext Transfer Protocol)

3. **What principle does a firewall use when there is no explicit rule for a certain type of traffic?**

    A. Least privilege

    B. Separation of duties

    C. Informed consent

    D. Implicit deny

4. **Which type of control is aimed at identifying potential security incidents after they occur?**

    A. Preventive

    B. Detective

    C. Corrective

    D. Deterrent

5. **Which of the following aims to manage and control risks in an organizational context?**

    A. Risk Governance

    B. Risk Evaluation

    C. Risk Planning

    D. Risk Treatment

6. **Which of the following is commonly used for providing an additional layer of security on wired networks?**

   A. WPA

   B. Firewall

   C. VPN

   D. Switch

7. **True or False: The vendor for PaaS is responsible for the hardware and data center.**

   A. True

   B. False

   C. Not applicable

   D. Depends on the contract

8. **Who should be consulted when developing an incident response plan?**

   A. ISO 27001

   B. NIST SP 800-53

   C. NIST SP 800-61

   D. ISO 31000

9. **What is ingress monitoring primarily concerned with?**

   A. Observing outgoing network communications

   B. Analyzing software application performance

   C. Monitoring incoming network traffic

   D. Managing network resource allocation

10. **What do guidelines refer to in security frameworks?**

   A. Mandatory Controls

   B. Best Practices

   C. Detailed Procedures

   D. Regulatory Requirements

Answers

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

Explanations

1. **What information security strategy integrates people, technology, and operations to establish security barriers?**

   A. Layered Security

   B. Defense in Depth

   C. Multi-Layered Protection

   D. Holistic Security Strategy

The term "Defense in Depth" refers to a comprehensive information security strategy that employs multiple layers of defense across physical, technical, and administrative controls. The concept is predicated on the idea that a successful security posture cannot rely on a single security measure; rather, it must integrate various overlapping techniques that create "barriers" to potential threats. This strategy recognizes that threats can emerge from multiple vectors—such as external attackers, insider threats, and even unintentional actions by users. By implementing layered defenses, organizations can slow down or deter an attack, providing additional time to detect and respond to security incidents. Each layer serves a distinct function and utilizes different technologies, policies, and practices, ensuring there are several hurdles a threat must overcome before achieving its objective. Other options may incorporate elements of security but don't provide the same comprehensive and strategic approach to integrating people, technology, and operations. For example, "Layered Security" is technically similar but may not emphasize the holistic integration aspect as strongly as "Defense in Depth." "Multi-Layered Protection" tends to emphasize the number of layers rather than the effective integration of those layers into a cohesive strategy. "Holistic Security Strategy" suggests a more encompassing view but does not specifically convey the structured, tier

2. **Which protocol would help synchronize devices within a company's internal IT environment?**

   A. FTP (File Transfer Protocol)

   B. NTP (Network Time Protocol)

   C. SMTP (Simple Mail Transfer Protocol)

   D. HTTP (Hypertext Transfer Protocol)

NTP, or Network Time Protocol, is specifically designed to synchronize the clocks of computers and other devices across a network. Accurate timekeeping is vital for various network functions, including logging events, scheduling tasks, and running applications that depend on time-sensitive operations. By ensuring that all devices within a company's internal IT environment have synchronized time, NTP helps prevent discrepancies that could lead to issues in data integrity, system performance, and security. In contrast, FTP is primarily used for transferring files between systems, SMTP handles the sending of emails, and HTTP is focused on delivering web content. While these protocols play critical roles in their respective domains, they do not provide the functionality required to synchronize devices' clocks or maintain time accuracy across an internal network. Therefore, NTP is the essential protocol for achieving synchronization within an organization's IT environment.

3. What principle does a firewall use when there is no explicit rule for a certain type of traffic?

A. Least privilege

B. Separation of duties

C. Informed consent

D. Implicit deny

A firewall operates on the principle of implicit deny when it encounters traffic for which there is no explicit rule defined. This principle dictates that any traffic that is not explicitly allowed by a rule is automatically denied. The concept is built on the assumption that unless there is a clear permission in place, the default reaction is to block the traffic. This presumption enhances security by limiting exposure to potential threats. By denying traffic that hasn't been explicitly permitted, firewalls help protect networks from unauthorized access and attacks that exploit unfiltered data flows. This strategy is crucial for preventing any unintended access or communication that could harm a system or compromise sensitive data. The other principles listed—like least privilege, separation of duties, and informed consent—either focus on reducing unnecessary permissions, ensuring that roles and responsibilities are clearly defined, or obtaining user agreement, respectively, but they do not directly address how firewalls handle traffic that lacks explicit authorization.

4. Which type of control is aimed at identifying potential security incidents after they occur?

A. Preventive

B. Detective

C. Corrective

D. Deterrent

The choice that focuses on identifying potential security incidents after they occur is known as detective controls. These controls are specifically designed to monitor systems and networks to detect and alert on unauthorized access or anomalies after they have happened. The primary goal of detective controls is to provide timely information about security incidents so that organizations can respond appropriately. Common examples include intrusion detection systems, security information and event management (SIEM) systems, and log analysis. Preventive controls focus on stopping potential security incidents before they happen, such as firewalls and access controls. Corrective controls come into play after an incident has been identified, aiming to rectify or mitigate the damage caused. Deterrent controls are designed to discourage potential attackers from attempting an attack in the first place, often through visible security measures or policies. Thus, the focus of detective controls on post-incident identification distinguishes them clearly from these other types of controls.

5. Which of the following aims to manage and control risks in an organizational context?

A. Risk Governance

B. Risk Evaluation

C. Risk Planning

D. Risk Treatment

The correct response focuses on the concept of risk governance, which involves the framework and processes that organizations use to identify, manage, and control risks. It encompasses the overall management approach to risk, establishing roles and responsibilities, policies, and procedures to ensure that risk management is integrated into the organization's culture and operations. Effective risk governance enables organizations to proactively address potential risks, ensuring that they align with their strategic objectives and comply with regulatory requirements. Risk evaluation, while important, is a specific process within the broader risk management framework. It focuses primarily on assessing the likelihood and impact of identified risks, rather than the overarching system that governs how those risks are managed. Similarly, risk planning deals with the processes involved in developing a strategy for responding to risks but does not encompass the governance aspect. Risk treatment, on the other hand, pertains to the options available for managing identified risks, such as avoidance, mitigation, transfer, or acceptance, without addressing the governance structure that supports these actions.

6. Which of the following is commonly used for providing an additional layer of security on wired networks?

A. WPA

B. Firewall

C. VPN

D. Switch

A firewall serves an essential function in enhancing security on wired networks by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, effectively reducing the risk of unauthorized access, attacks, and data breaches. Firewalls can be implemented as hardware devices or software applications, allowing organizations to establish a secure perimeter around their network. They can filter traffic, block malicious content, and prevent harmful communications, thereby offering a robust line of defense. In contrast, while other options might provide security aspects—WPA is primarily associated with securing wireless networks, VPNs enhance security for remote connections, and switches are mainly concerned with directing network traffic rather than securing it—none of them offer the same level of protective measures specifically tailored for wired environments as a firewall does. Therefore, the correct response highlights the critical role that firewalls hold in maintaining the integrity and security of wired networks.

7. True or False: The vendor for PaaS is responsible for the hardware and data center.

A. True

B. False

C. Not applicable

D. Depends on the contract

In a Platform as a Service (PaaS) model, the vendor indeed takes responsibility for the underlying hardware and the data center infrastructure. This includes the physical servers, storage, and networking resources necessary to run the PaaS environment. By using PaaS, developers can focus on building, testing, and deploying applications without having to manage the infrastructure themselves. The vendor provides the platform and tools required for application development, thereby abstracting away the complexities associated with hardware management, data center operations, and maintenance. This division of responsibilities allows users to benefit from a more streamlined approach to application development, as the vendor handles aspects such as hardware provisioning, maintenance, and scalability. Therefore, stating that the vendor for PaaS is responsible for the hardware and data center is accurate, making the statement true.

8. Who should be consulted when developing an incident response plan?

A. ISO 27001

B. NIST SP 800-53

C. NIST SP 800-61

D. ISO 31000

Consulting NIST SP 800-61 when developing an incident response plan is particularly relevant because this publication specifically focuses on computer security incident handling. It provides guidelines on how organizations can respond to incidents effectively, which includes preparing for incidents, detecting and analyzing them, and ultimately responding to and recovering from them. This tailored guidance is essential for creating a robust incident response plan that aligns with best practices in cybersecurity. The other options, while valuable in their own right, do not specifically address the incident response process in the same manner. ISO 27001 provides a framework for establishing, implementing, and managing an information security management system (ISMS), which is broader than the specific scope of incident response. NIST SP 800-53 offers a catalog of security and privacy controls for federal information systems and organizations, focusing more on organizational security practices rather than specific incident response strategies. ISO 31000 focuses on risk management principles and guidelines that can apply across any domain but do not pertain specifically to incident response plans. Thus, NIST SP 800-61 stands out as the most pertinent resource for this purpose.

9. What is ingress monitoring primarily concerned with?

A. Observing outgoing network communications

B. Analyzing software application performance

C. Monitoring incoming network traffic

D. Managing network resource allocation

Ingress monitoring is primarily concerned with monitoring incoming network traffic. This involves analyzing and recording data packets that enter a network from external sources. The goal is to detect any unusual activity, identify potential threats, and ensure that the network's security policies are being upheld. By monitoring this inbound traffic, organizations can establish baselines for normal activity and quickly spot anomalies that may indicate security breaches or attempts at unauthorized access. Ingress monitoring plays a crucial role in safeguarding a network by providing insights into what types of traffic are allowed and what malicious activities might be attempting to penetrate the perimeter. This proactive approach helps in assessing threats in real time and can trigger alerts or automated responses to mitigate risks. On the other hand, analyzing software application performance pertains to the efficiency and usability of software systems rather than network traffic. Observing outgoing communications focuses on data leaving the network, which does not include ingress monitoring. Lastly, managing network resource allocation is about optimizing the distribution of network resources for performance, not directly related to monitoring incoming traffic.

10. What do guidelines refer to in security frameworks?

A. Mandatory Controls

B. Best Practices

C. Detailed Procedures

D. Regulatory Requirements

Guidelines within security frameworks typically refer to recommended best practices that organizations can implement to enhance their security posture. These best practices are not mandatory but serve as valuable advice based on industry standards, expert consensus, and lessons learned from previous incidents. They assist organizations in making informed decisions about securing their systems and data, while also providing flexibility to tailor the recommendations to their specific environment and risk level. In contrast, other categories such as mandatory controls refer to specific security measures that must be followed, which often stem from regulatory requirements. Detailed procedures provide step-by-step instructions for executing tasks within the framework, while regulatory requirements encompass laws and standards that organizations must comply with to avoid legal penalties or fines. Best practices, however, stand out as guidance that can lead to improved security outcomes without the obligation of strict adherence.

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://isc2certifiedincybersecurity.examzify.com

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