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

Study Guide

Everything you need from our exam experts!

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. Which procedure is crucial in managing security incidents?

- **A. Data encryption**
- **B. Patching software regularly**
- **C. Creating an Incident Response Plan**
- **D. Limiting internet access**

2. What type of control is designed to identify security issues that necessitate further investigation?

- **A. Preventive Control**
- **B. Detective Control**
- **C. Recovery Control**
- **D. Comprehensive Control**

3. What does a security vulnerability management program focus on?

- **A. Identifying and prioritizing security vulnerabilities**
- **B. Developing strong encryption protocols**
- **C. Enhancing user access control**
- **D. Standardizing incident response procedures**

4. In a scenario where Joe conducts full backups on Sunday and incremental backups during the week, what backups are needed after a failure on Friday morning?

- **A. Only Thursday's backup**
- **B. Sunday's full backup and all incremental backups from Monday to Thursday**
- **C. Only the last backup**
- **D. Sunday's full backup and Thursday's differential backup**

5. What best describes a cold site in disaster recovery?

- **A. Fully equipped with servers and ready to go**
- **B. Empty except for core infrastructure**
- **C. Operational within a few hours**
- **D. Has online and offline backups**

6. What technique is often employed to verify data integrity?

A. Data compression

B. Checksum calculation

C. File fragmentation

D. Data duplication

7. Which process begins after an incident response is initiated?

A. Incident Auditing

B. Evidence Gathering

C. Damage Assessment

D. Documentation Review

8. What port range is known as the "well-known" ports?

A. 0 - 1,023

B. 0 - 1,000

C. 0 - 10,000

D. 0 - 65,535

9. Which process is essential for maintaining security and effectiveness against attacks?

A. Annual budgeting

B. Conferences with senior leadership

C. Updating and patching systems

D. The annual shareholders' meeting

10. What type of disaster recovery site can be activated the most quickly in the event of a disruption?

A. Cold site

B. Warm site

C. Hot site

D. Backup site

Answers

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

Explanations

1. Which procedure is crucial in managing security incidents?

A. Data encryption

B. Patching software regularly

C. Creating an Incident Response Plan

D. Limiting internet access

Creating an Incident Response Plan is fundamental in managing security incidents because it provides a structured approach to identifying, responding to, and recovering from security incidents. An effective incident response plan outlines the processes and protocols that an organization should follow when a security breach occurs. This plan typically includes defining roles and responsibilities, communication strategies, methods for containing and mitigating incidents, and steps for eradicating threats. By having a pre-defined plan, organizations can react swiftly and effectively, reducing the potential impact of security incidents and minimizing downtime. Although data encryption, patching software regularly, and limiting internet access are important security practices, they serve primarily as preventive controls that help to mitigate the risk of incidents rather than manage them in the event they occur. The incident response plan specifically addresses how to handle situations after a security breach has been detected, making it a crucial component of an organization's overall cybersecurity strategy.

2. What type of control is designed to identify security issues that necessitate further investigation?

A. Preventive Control

B. Detective Control

C. Recovery Control

D. Comprehensive Control

Detective control is designed to identify security issues, allowing organizations to recognize potential breaches or anomalies after they have occurred. This type of control plays a critical role in incident response, as it provides the necessary information to investigate and respond to security threats effectively. For example, systems like intrusion detection systems (IDS) monitor activities on a network to identify unauthorized access or unusual behavior. Logs and alerts generated by these systems can indicate potential security events that require further examination. By detecting and alerting on these issues, organizations can take timely action to mitigate risks and enhance their security posture. In contrast, preventive controls aim to stop security incidents from occurring in the first place, while recovery controls focus on restoring systems after an incident has taken place. Comprehensive control isn't commonly defined in cybersecurity contexts and doesn't specifically pertain to identifying issues needing investigation. Thus, the focus on detection and investigation aligns precisely with the purpose of detective controls.

3. What does a security vulnerability management program focus on?

A. Identifying and prioritizing security vulnerabilities

B. Developing strong encryption protocols

C. Enhancing user access control

D. Standardizing incident response procedures

A security vulnerability management program primarily focuses on identifying and prioritizing security vulnerabilities. This process is critical because it helps organizations systematically discover weaknesses in their systems, applications, and infrastructure that could be exploited by attackers. By identifying these vulnerabilities, the program allows an organization to assess which vulnerabilities pose the most significant risk based on various factors, such as the potential impact of exploitation and the likelihood of occurrence. Once vulnerabilities are identified, they can be prioritized for remediation based on their severity and the organization's risk appetite. This prioritization ensures that resources are allocated effectively to address the most pressing vulnerabilities first, which is essential for maintaining a robust security posture. Developing strong encryption protocols, enhancing user access control, and standardizing incident response procedures are important aspects of an organization's security strategy but do not directly pertain to the core objectives of a vulnerability management program. These elements may support the overall security framework but are not the specific focus of a vulnerability management initiative.

4. In a scenario where Joe conducts full backups on Sunday and incremental backups during the week, what backups are needed after a failure on Friday morning?

A. Only Thursday's backup

B. Sunday's full backup and all incremental backups from Monday to Thursday

C. Only the last backup

D. Sunday's full backup and Thursday's differential backup

In this scenario, Joe's backup strategy involves performing a full backup on Sundays and incremental backups throughout the week. An incremental backup saves only the data that has changed since the last backup, which means that each incremental backup relies on the previous backup for completeness. In the event of a failure on Friday morning, recovery requires the latest full backup along with all subsequent incremental backups taken since that last full backup. Therefore, the restoration process would need: 1. The full backup from Sunday. This contains all the data as of that point in time. 2. The incremental backups from Monday, Tuesday, Wednesday, and Thursday, which contain only the changes made since the last backup (in this case, the last full backup on Sunday). Thus, the correct approach to restoring data after the failure would require all these backups in sequence. By only restoring Sunday's full backup and all incremental backups from Monday to Thursday, all required data will be recovered to a point right before the failure occurred on Friday morning, aligning perfectly with Joe's backup schedule. Other options, such as retrieving only Thursday's backup or just the last backup, would not provide a complete recovery of data. A differential backup, which is not in Joe's stated strategy, would also not correctly represent the

5. What best describes a cold site in disaster recovery?

A. Fully equipped with servers and ready to go

B. Empty except for core infrastructure

C. Operational within a few hours

D. Has online and offline backups

A cold site in disaster recovery refers to a location that is empty except for core infrastructure, such as basic power, cooling, and network connectivity. This site is not equipped with the necessary servers and technology to immediately take over business operations in the event of a disaster. Instead, a cold site serves as a backup facility that organizations can utilize to set up their operations after a disaster occurs. The full setup of systems and data restoration must take place before the site can become operational. The primary characteristic that distinguishes a cold site is its lack of pre-installed hardware, which means that organizations must bring in all the necessary equipment and restore data from backups to resume full operations. This typically involves more time and effort, making it ideal for organizations that prioritize cost over recovery speed. In contrast, a fully equipped site would be referred to as a hot site, which is ready to go immediately. An operational site within a few hours suggests a warm site, which has some equipment and may have data replication in place, but is not as fully remote and prepared as a hot site. Online and offline backups pertain to data availability rather than the physical nature of the disaster recovery site itself.

6. What technique is often employed to verify data integrity?

A. Data compression

B. Checksum calculation

C. File fragmentation

D. Data duplication

Calculating a checksum is an essential technique used to verify data integrity. A checksum is a value derived from the content of a data set through a mathematical operation, typically involving hashing algorithms. When data is transmitted or stored, a checksum is computed and usually sent or stored alongside the data. Upon retrieval or after transmission, the checksum is recalculated. If the newly calculated checksum matches the original, it indicates that the data has remained unchanged and intact. On the other hand, if there is a discrepancy, it suggests potential data corruption, tampering, or transmission errors. This method is widely used in various applications, such as file transfers, data storage, and network protocols, to ensure that the data remains pure and unaltered over time. The other techniques mentioned do not focus on verifying data integrity in the same direct manner. Data compression reduces the size of data without being inherently designed to check for changes in the data itself. File fragmentation divides files into smaller pieces for storage efficiency, and while it can relate to data management, it doesn't verify integrity. Data duplication aims to create copies of data for backup and redundancy purposes, but it does not inherently ensure that the original and duplicate copies are identical unless paired with an integrity check method like checksums.

7. Which process begins after an incident response is initiated?

A. Incident Auditing

B. Evidence Gathering

C. Damage Assessment

D. Documentation Review

The process that begins after an incident response is initiated is damage assessment. This phase is critical as it helps identify the impact of the incident on the organization's systems, data, and operations. Damage assessment involves evaluating the extent of the compromise, understanding how it occurred, and determining which assets were affected. This process is essential for formulating an effective recovery strategy, communicating with stakeholders, and ensuring that necessary remedial actions are taken to prevent future incidents. It lays the foundation for prioritizing responses and resource allocation based on the level of damage incurred. Further steps, such as evidence gathering, documentation review, or incident auditing, may follow, but they typically rely on the insights gained during the damage assessment phase. Therefore, the accurate recognition of the sequence of these processes is vital for effective incident management and mitigation.

8. What port range is known as the "well-known" ports?

A. 0 - 1,023

B. 0 - 1,000

C. 0 - 10,000

D. 0 - 65,535

The port range defined as "well-known" ports is from 0 to 1,023. This range is used by many popular protocols and services, including HTTP (port 80), FTP (port 21), and SMTP (port 25). These ports are established and assigned by the Internet Assigned Numbers Authority (IANA) for standard services and are recognized across all systems for network communications. Ports in this range are reserved for system or administrative purposes and require elevated privileges for applications to bind to them. This standardization is essential for ensuring consistent operation across various platforms and services, as it enables applications to reliably connect using commonly recognized ports. The other ranges mentioned, such as 0-1,000 or 0-10,000, extend beyond the defined well-known range, while the range 0-65,535 encompasses all possible ports, including both well-known ports and registered or dynamic ports. Thus, the correct identification of the well-known port range is crucial for understanding networking and cybersecurity fundamentals.

9. Which process is essential for maintaining security and effectiveness against attacks?

A. Annual budgeting

B. Conferences with senior leadership

C. Updating and patching systems

D. The annual shareholders' meeting

Maintaining security and effectiveness against attacks requires a proactive approach to managing vulnerabilities in information systems. Updating and patching systems is a critical process because it addresses known security flaws in software and hardware. Cybercriminals frequently exploit these vulnerabilities, and failure to apply updates can leave systems susceptible to various attacks, such as malware infections, data breaches, or ransomware. When organizations regularly update and patch their systems, they strengthen their overall security posture. This ensures that they benefit from the latest security enhancements, bug fixes, and protection mechanisms provided by software vendors. In addition, timely updates can mitigate risks associated with zero-day vulnerabilities, which are exploited by attackers shortly after they are discovered. The other options, while important in their own contexts, do not have the same direct impact on immediate security against cyber threats. Annual budgeting and conferences with senior leadership are more focused on planning and decision-making processes rather than on actively mitigating security risks. The annual shareholders' meeting is primarily concerned with organizational performance and shareholder interests, which may not directly relate to the day-to-day operational security of systems.

10. What type of disaster recovery site can be activated the most quickly in the event of a disruption?

A. Cold site

B. Warm site

C. Hot site

D. Backup site

The most suitable type of disaster recovery site that can be activated the quickest during a disruption is a hot site. A hot site is fully operational and equipped with the necessary hardware, software, and data required to continue business operations almost immediately after a disaster occurs. It typically mirrors the primary site in real-time, ensuring that the data is current and that systems are ready to be used without significant delay. In contrast, a cold site has minimal equipment and requires significant time to set up systems and restore data, making it unsuitable for rapid recovery. A warm site sits in the middle; it has some hardware and may have data backups in place, but it still requires setup and synchronization before being fully operational. While a backup site can refer to various options for data recovery or system restoration, it does not specifically denote a site that is immediately ready for activation like a hot site. Therefore, for organizations prioritizing minimal downtime and quick restoration of operations, a hot site is the optimal choice.

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!