ISACA CYBERSECURITY FUNDAMENTALS CERTIFICATION PRACTICE EXAM (SAMPLE)

STUDY GUIDE

Prepare with structure. Pass with confidence

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

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 of the following describes a "Security Perimeter"?**
   A. A boundary that defines secure areas
   B. A static point of access in a network
   C. A well-defined boundary between the organization and the outside world
   D. An unrestricted zone around the organization

2. **What is the main goal of the System Development Life Cycle (SDLC)?**
   A. To create user manuals for systems
   B. To plan, create, test, and deploy information systems
   C. To ensure user compliance with policies
   D. To manage system installations

3. **Which of the following can be considered a privileged service?**
   A. Email services
   B. File transfers
   C. HTTP services on port 80
   D. Streaming services

4. **What is a packet-filtering firewall primarily designed to do?**
   A. Track user behavior
   B. Examine each packet for passage determination
   C. Encrypt data packets
   D. Prevent all forms of traffic

5. **What characterizes script kiddies in the context of threat agents?**
   A. They are experienced hackers
   B. They use existing tools for learning without full understanding
   C. They target corporate networks for profit
   D. They coordinate organized campaigns

6. **What does data in transit refer to?**
   A. Data that is stored in databases
   B. Data traveling over a network
   C. Data that is currently being processed
   D. Data that is backed up

7. Which of the following is a key component of developing a Business Impact Analysis (BIA)?

A. Assessing the organization's financial records

B. Identifying business processes of strategic importance

C. Designing social media strategies

D. Creating a marketing plan for products

8. What function does a Web-application firewall perform?

A. It provides encryption for all web traffic

B. It applies rules to a specific web application at the OSI model's higher level

C. It acts as a backup for web server data

D. It serves as a basic access control for all devices

9. What is essential for ensuring the integrity of evidence during cybersecurity investigations?

A. Effective incident response planning

B. Proper investigator skills and experiences

C. Regular system audits

D. Maintaining a detailed chain of custody

10. What range of port numbers is considered 'well known'?

A. 49152 to 65535

B. 1024 to 49151

C. 0 to 1023

D. 256 to 512

Answers

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

Explanations

1. Which of the following describes a "Security Perimeter"?

A. A boundary that defines secure areas

B. A static point of access in a network

C. A well-defined boundary between the organization and the outside world

D. An unrestricted zone around the organization

A "Security Perimeter" is best described as a well-defined boundary between the organization and the outside world. This concept is central to cybersecurity as it establishes where the security protocols and controls are applied. By delineating this boundary, organizations can implement various security measures such as firewalls, intrusion detection systems, and access controls to protect internal assets from external threats. The essence of a security perimeter is to create a clear demarcation between trusted internal networks and untrusted external environments. This helps in identifying what traffic is allowed through the perimeter and ensures that only authorized users and data can access sensitive information within the organization. Understanding this boundary is crucial for assessing vulnerabilities and implementing security policies effectively. In the context of the other options, while a boundary that defines secure areas (the first option) has some relevance, it lacks the specificity of delineating between internal and external contexts. A static point of access in a network implies a fixed location rather than an encompassing security strategy. An unrestricted zone around the organization contradicts the very purpose of a security perimeter, which seeks to restrict access and protect against external vulnerabilities.

2. What is the main goal of the System Development Life Cycle (SDLC)?

A. To create user manuals for systems

B. To plan, create, test, and deploy information systems

C. To ensure user compliance with policies

D. To manage system installations

The primary goal of the System Development Life Cycle (SDLC) is to provide a structured framework for planning, creating, testing, and deploying information systems. This methodology ensures that systems are developed in a systematic way, allowing for thorough analysis and documentation at each stage of the process. By following the SDLC, organizations can better manage the complexities and potential risks associated with system development. The various phases—such as requirement gathering, design, implementation, and testing—ensure that the end product meets the intended purpose, is of high quality, and satisfies user needs. Each phase has specific deliverables and processes that contribute to the overall success of the information system. While creating user manuals, ensuring user compliance, and managing installations are important aspects of systems management, they support the broader framework but do not reflect the overall goal of the SDLC itself. The emphasis on a comprehensive approach to system development encapsulates the essence of what the SDLC aims to achieve.

3. Which of the following can be considered a privileged service?

A. Email services

B. File transfers

C. HTTP services on port 80

D. Streaming services

The correct choice refers to HTTP services on port 80 as a privileged service because it is a well-known protocol commonly used for web traffic. In the context of cybersecurity, "privileged services" often implies services that handle sensitive data or are critical for communication and access in a networked environment. HTTP is foundational for web applications, including those that require secure transactions, which can involve confidential user information. Privileged services, as a category, include those that have elevated access within the network architecture or that can interact with other services in a way that requires special privileges due to the nature of the data they transmit or the operations they perform. Since HTTP on port 80 is crucial for delivering web content, it can be seen as requiring a certain level of privilege and security oversight. In contrast, while email services, file transfers, and streaming services may handle data, they typically operate under different layers of protocol and do not inherently denote the same level of privilege. Email services often function on various designated ports that may not require elevated privileges as part of their standard operation; file transfers can utilize FTP or other protocols which might not have the same level of oversight; and streaming services are more focused on media delivery which does not necessitate the same access considerations as web

4. What is a packet-filtering firewall primarily designed to do?

A. Track user behavior

B. Examine each packet for passage determination

C. Encrypt data packets

D. Prevent all forms of traffic

A packet-filtering firewall is primarily designed to examine each packet that attempts to pass through it and determine whether to allow or block that packet based on pre-defined security rules. This process involves analyzing attributes such as source and destination IP addresses, protocol types, and port numbers, enabling the firewall to make informed decisions about whether a packet complies with the organization's security policies. The primary purpose of packet filtering is to create a barrier between a trusted internal network and untrusted external networks, such as the Internet, without the complexity or overhead associated with more advanced firewall techniques. By filtering traffic at a packet level, this type of firewall can efficiently allow legitimate traffic while blocking unauthorized access or potentially harmful transmissions. In contrast, tracking user behavior focuses on monitoring and analyzing individual user activities rather than packets of data. Encrypting data packets pertains to securing data in transit by converting it into an unreadable format, which is a different function that packet-filtering firewalls do not perform. Preventing all forms of traffic would defeat the primary role of a firewall, which is to regulate and control traffic rather than block it entirely.

5. What characterizes script kiddies in the context of threat agents?

A. They are experienced hackers

B. They use existing tools for learning without full understanding

C. They target corporate networks for profit

D. They coordinate organized campaigns

Script kiddies are typically characterized by their reliance on pre-existing scripts and tools to conduct their activities rather than developing their own techniques or fully understanding the underlying systems they exploit. This group often lacks the deep technical knowledge and experience that seasoned hackers possess. They tend to use readily available software and exploits to test their abilities or conduct attacks, primarily motivated by the desire for notoriety or thrill rather than financial gain or significant malicious intent. In contrast, experienced hackers develop sophisticated tools and have a comprehensive knowledge of hacking principles. Those who target corporate networks for profit usually have specific goals and a deeper understanding of their initiatives, while organized campaigns suggest coordination and strategic planning which go beyond the often spontaneous actions of script kiddies. Therefore, the characterization of script kiddies accurately reflects their reliance on accessible resources without an inherent understanding of the complexities of cybersecurity.

6. What does data in transit refer to?

A. Data that is stored in databases

B. Data traveling over a network

C. Data that is currently being processed

D. Data that is backed up

Data in transit refers to information that is actively moving from one location to another, typically over a network. This movement can occur between devices, such as when a user sends an email or when data is transmitted between servers. It is crucial to protect data in transit because it is vulnerable to interception, which can lead to unauthorized access or data breaches. To safeguard this type of data, various security measures such as encryption protocols (e.g., TLS/SSL) can be implemented, ensuring that even if the data is intercepted, it cannot be easily read or misused. In contrast, the other options describe different states or conditions of data. Data stored in databases pertains to data that resides at rest, not in motion. Data that is currently being processed refers to active data in use but not necessarily moving over a network. Data that is backed up involves copies of data saved for disaster recovery purposes, again not relevant to the concept of data in transit. Collectively, these distinctions highlight why identifying data in transit is essential for implementing appropriate cybersecurity measures.

7. Which of the following is a key component of developing a Business Impact Analysis (BIA)?

A. Assessing the organization's financial records

B. Identifying business processes of strategic importance

C. Designing social media strategies

D. Creating a marketing plan for products

Identifying business processes of strategic importance is a key component of developing a Business Impact Analysis (BIA) because the primary purpose of a BIA is to determine the potential effects of a disruption on an organization's operations, revenue, reputation, and overall viability. By identifying these critical business processes, organizations can assess which functions are vital to their success and continuity. This step allows decision-makers to prioritize resources and recovery efforts to ensure that the most essential services can be resumed quickly in the event of a disruption. Focusing on strategic business processes also helps in understanding dependencies between different functions and the potential cascade effects of disruptions. It provides a comprehensive understanding of how various elements of the organization interact, which is essential for informed planning and risk management. The other options do not directly address the core objectives of a BIA. For example, assessing financial records may provide useful information but does not focus specifically on the impact of business disruptions. Social media strategies and marketing plans, while important for overall business strategy, do not contribute directly to understanding the impacts of potential disruptions on key business functions. Therefore, the correct choice emphasizes the necessity of pinpointing vital processes for effective business continuity planning.

8. What function does a Web-application firewall perform?

A. It provides encryption for all web traffic

B. It applies rules to a specific web application at the OSI model's higher level

C. It acts as a backup for web server data

D. It serves as a basic access control for all devices

The role of a Web Application Firewall (WAF) is to protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It is specifically designed to understand and enforce rules at higher levels of the OSI model, particularly Layer 7, which pertains to the application layer. By applying a set of predefined rules, a WAF can effectively analyze incoming requests and outgoing responses for malicious content, such as SQL injections, cross-site scripting (XSS), and other web application vulnerabilities. This function is crucial for defending against common attack types that specifically target application flaws, thus ensuring the security of the web application itself. Considering the other options, while encryption for web traffic is indeed an important security measure, it does not encapsulate the primary function of a WAF. Backup for web server data is an entirely separate function that relates more to data recovery and availability than security. Basic access control for devices pertains to network level security rather than the application level, which is the domain of a WAF, confirming that option specific to setting application-level rules is indeed the most accurate.

9. What is essential for ensuring the integrity of evidence during cybersecurity investigations?

A. Effective incident response planning

B. Proper investigator skills and experiences

C. Regular system audits

D. Maintaining a detailed chain of custody

Maintaining a detailed chain of custody is crucial for ensuring the integrity of evidence during cybersecurity investigations. The chain of custody refers to the process of maintaining and documenting the handling of evidence from the moment it is collected until it is presented in court. This involves recording who collected the evidence, how it was collected, where it was stored, who had access to it, and how it was transported. This meticulous documentation is vital because it establishes the authenticity of the evidence and ensures that it has not been altered or tampered with at any point in the investigation. If evidence cannot be verified due to a broken chain of custody, it may be deemed inadmissible in a legal setting, which can jeopardize the entire investigation. Therefore, having a well-documented chain of custody preserves the integrity of the evidence and supports its reliability in legal or judicial proceedings. While effective incident response planning, proper investigator skills, and regular system audits contribute to overall cybersecurity practices and can assist in an investigation, they do not specifically guarantee the integrity of the evidence itself. The chain of custody uniquely addresses the continuity and preservation of the evidence's integrity throughout the investigative process.

10. What range of port numbers is considered 'well known'?

A. 49152 to 65535

B. 1024 to 49151

C. 0 to 1023

D. 256 to 512

The range of port numbers classified as 'well known' is from 0 to 1023. These ports are designated for specific services and protocols, meaning they are reserved for well-known applications and processes. For instance, port 80 is used for HTTP, port 443 for HTTPS, and port 25 for SMTP. Well-known ports facilitate the identification of specific services, enabling standardized communication across the internet and ensuring that when a client attempts to communicate with a server, it knows which service it should address based on the port number being used. In contrast, the other ranges mentioned are categorized differently. Ports from 1024 to 49151 are known as 'registered' ports, typically assigned by IANA (Internet Assigned Numbers Authority) for user processes or applications. The range from 49152 to 65535 is referred to as 'dynamic or private' ports, which are usually ephemeral and can be used temporarily by applications when they initiate a connection. The range from 256 to 512 does not fit into any standard classification of port numbers.

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://isaca-cybersecurity.examzify.com

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