HITRUST CERTIFIED COMMON SECURITY FRAMEWORK PRACTITIONER (CCSFP) PRACTICE EXAM (SAMPLE)

STUDY GUIDE

Prepare with structure. Pass with confidence

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. **What is the minimum score required for an organization to achieve certification in an i1 assessment?**

   A. 60

   B. 70

   C. 75

   D. 83

2. **Which of the following is NOT considered a type of evidence in an audit?**

   A. Verbal information

   B. Testimony from employees

   C. Electronic information

   D. Paper documents

3. **Is it true that any relying party can be invited to review assessment results in the RDS?**

   A. True

   B. False

   C. Only certified assessors can review

   D. Only authorized users can review

4. **Which trust service principles have been mapped by HITRUST CSF?**

   A. Confidentiality, Integrity, Availability

   B. Security, Availability, Confidentiality

   C. Access, Integrity, Security

   D. Confidentiality, Availability, Integrity

5. **What must the test plan address according to HITRUST guidelines?**

   A. Overall security strategy

   B. Each Requirement Statement

   C. Management reviews

   D. Quality assurance methods

6. How must the procedures be structured for compliance assessments?

A. To be lengthy and comprehensive

B. At a sufficient level of detail

C. To require expert knowledge only

D. To include irrelevant information

7. Which assessment allows for the highest percentage of control inheritance from cloud service providers?

A. i1 Validated Assessment

B. r2 Validated Assessment

C. e1 Validated Assessment

D. All allow the same

8. How long is a CCSFP license valid, provided annual refresher training is taken?

A. 1 year

B. 2 years

C. 3 years

D. 5 years

9. What does "Non-Compliant" indicate in the maturity levels?

A. 0% compliance coverage

B. 25% compliance coverage

C. 50% compliance coverage

D. 75% compliance coverage

10. What is the main function of the HITRUST Common Security Framework?

A. Provide a guideline for risk assessment

B. Serve as a framework for health information security

C. Establish a set of national security standards

D. Ensure only technical compliance

Answers

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

Explanations

1. What is the minimum score required for an organization to achieve certification in an i1 assessment?

A. 60

B. 70

C. 75

D. 83

To achieve certification in an i1 assessment under the HITRUST framework, an organization must attain a minimum score of 83. This threshold is set to ensure that organizations not only comply with basic requirements but also demonstrate a higher level of security program maturity and effectiveness. The i1 assessment encompasses a broader assessment of controls compared to lower scoring benchmarks, and meeting or exceeding this score reflects that the organization has implemented appropriate security practices to protect sensitive information. Thus, achieving a score of 83 signifies a commitment to maintaining robust security standards, which is crucial for gaining HITRUST certification and instilling confidence in stakeholders regarding the organization's ability to manage risk and protect data responsibly.

2. Which of the following is NOT considered a type of evidence in an audit?

A. Verbal information

B. Testimony from employees

C. Electronic information

D. Paper documents

Testimony from employees can actually serve as a form of evidence in an audit, as it reflects firsthand accounts and observations that can be valuable in evaluating compliance and understanding processes. Therefore, this option is not the one that fails to qualify as evidence. The correct interpretation should focus on the notion that verbal information, even if it is provided during an audit, typically lacks the formal documentation that is necessary to substantiate claims or findings. In auditing terms, tangible or recorded evidence is vital to forming reliable conclusions, and the other options—electronic information and paper documents—are considered robust types of evidence because they can be recorded and reviewed, which supports their validity and reliability in an audit context. Hence, while verbal communication and testimony can inform the audit process, it does not hold the same evidential weight as tangible forms of evidence like electronic records or paper documents.

3. Is it true that any relying party can be invited to review assessment results in the RDS?

A. True

B. False

C. Only certified assessors can review

D. Only authorized users can review

The statement is accurate because the HITRUST Relying Party Directory (RDS) is designed to facilitate transparency and collaboration between organizations that have undergone HITRUST assessments and those that rely on the results of these assessments. The intention is to promote trust and understanding in the security posture of assessed organizations. Inviting any relying party to review the assessment results allows these parties to make informed decisions about the security and compliance capabilities of the organization being assessed. This openness not only fosters accountability but also enhances the overall effectiveness of the HITRUST certification process, as it allows stakeholders, including third-party entities that may work with the certified organization, to understand the context and depth of the assessments conducted. Others might assert that there are restrictions on who can view assessment results, but access for relying parties is intentionally broad to promote confidence in the HITRUST Framework and to support the operational relationships between organizations in a risk-managed environment. By allowing any relying party to review results, the RDS strengthens the collaborative approach to security compliance without enforcing unnecessary barriers.

4. Which trust service principles have been mapped by HITRUST CSF?

A. Confidentiality, Integrity, Availability

B. Security, Availability, Confidentiality

C. Access, Integrity, Security

D. Confidentiality, Availability, Integrity

*The correct choice identifies the trust service principles that HITRUST CSF has specifically mapped. HITRUST focuses on essential aspects of information security and data management through the principles of Security, Availability, and Confidentiality. - **Security** ensures that systems and data are protected against unauthorized access and breaches, which is foundational in managing risk and maintaining trust in the handling of sensitive information. - **Availability** guarantees that information and resources are accessible when needed, which is critical for maintaining operational effectiveness and meeting the needs of users and customers. - **Confidentiality** pertains to protecting sensitive information from unauthorized disclosure, ensuring that personal and organizational data remains private. These three principles are integral to the comprehensive security framework provided by HITRUST, emphasizing the importance of not only protecting data but also ensuring that it is available and secure at all times. Other combinations do not accurately reflect the principles specifically mapped by HITRUST, which is why they are not the correct answers.*

5. What must the test plan address according to HITRUST guidelines?

A. Overall security strategy

B. Each Requirement Statement

C. Management reviews

D. Quality assurance methods

The test plan must specifically address each Requirement Statement as outlined in the HITRUST framework. This is crucial because the Requirement Statements consist of various controls that are integral to maintaining compliance with the HITRUST Common Security Framework (CSF). By addressing each Requirement Statement in the test plan, organizations can ensure that they are systematically evaluating their security measures against established benchmarks, thereby identifying vulnerabilities or areas that need improvement. This approach not only helps in confirming that the organization adheres to industry standards but also provides a comprehensive view of the effectiveness of the implemented security controls. It allows organizations to validate that they are meeting not just the minimum necessary security requirements, but also effectively managing risks associated with the handling of sensitive data. A robust test plan that thoroughly covers each Requirement Statement ultimately supports the organization's efforts to achieve and maintain HITRUST certification, enhancing trust among stakeholders regarding data security practices.

6. How must the procedures be structured for compliance assessments?

A. To be lengthy and comprehensive

B. At a sufficient level of detail

C. To require expert knowledge only

D. To include irrelevant information

The procedures for compliance assessments must be structured at a sufficient level of detail to ensure that all relevant security controls and processes are effectively evaluated. This means that the assessment must have enough granularity to identify specific risks, gaps, and compliance requirements while remaining manageable and focused. Having a sufficient level of detail allows the assessors to discern compliance levels accurately, providing a clear understanding of which controls are effectively implemented and which require improvement. It facilitates a balanced approach where the depth of the assessment is adequate to draw meaningful conclusions without becoming excessively detailed to the point of being burdensome or unwieldy. The emphasis on sufficiency rather than length means that while comprehensive documentation can enhance the understanding of an organization's security posture, the primary goal is to achieve clarity and actionable insights that align with HITRUST standards. Thus, the focus is on what is necessary for a thorough and efficient compliance assessment, ensuring it is both relevant and effective.

7. Which assessment allows for the highest percentage of control inheritance from cloud service providers?

A. i1 Validated Assessment

B. r2 Validated Assessment

C. e1 Validated Assessment

D. All allow the same

The e1 Validated Assessment is designed to accommodate organizations that leverage cloud services extensively, allowing for a higher percentage of control inheritance from cloud service providers. This type of assessment recognizes the shared responsibility model inherent in cloud services, where certain security controls can be inherited from the cloud provider rather than implemented independently by the organization. This assessment approach is particularly advantageous for organizations that utilize various cloud services, as it enables them to effectively manage and assess their compliance by acknowledging the security measures already established by their providers. In this context, the e1 Validated Assessment not only streamlines the compliance process but also emphasizes the importance of collaboration with cloud providers in maintaining a robust security posture. While other assessment types exist, they do not generally permit the same level of control inheritance, as they may be tailored for organizations operating in more traditional IT environments or those with different compliance needs. Thus, the e1 Validated Assessment stands out for its suitability for cloud-focused compliance assessments, facilitating a more efficient path toward meeting HITRUST standards.

8. How long is a CCSFP license valid, provided annual refresher training is taken?

A. 1 year

B. 2 years

C. 3 years

D. 5 years

The duration of the CCSFP license validity is three years if the individual completes the required annual refresher training. This three-year period reflects the framework's commitment to keeping practitioners updated with the latest developments and best practices in cybersecurity. The annual refresher training is designed to reinforce essential knowledge and maintain competence in the field, ensuring that certified individuals are well-equipped to navigate the evolving landscape of information security. This training is a critical component of the certification, allowing professionals to stay informed about changes in regulations, threats, and technologies relevant to HITRUST and the broader cybersecurity arena. This structured approach emphasizes continuous learning and skill enhancement for CCSFP holders.

9. What does "Non-Compliant" indicate in the maturity levels?

A. 0% compliance coverage

B. 25% compliance coverage

C. 50% compliance coverage

D. 75% compliance coverage

In the context of maturity levels, "Non-Compliant" specifically indicates a scenario where there is a complete lack of compliance coverage, meaning 0% compliance coverage. This reflects an organization's failure to meet any of the specified requirements within the framework. Achieving "Non-Compliant" status underscores that the necessary controls and practices are not in place to address the relevant security and privacy requirements. This level highlights a significant gap in compliance and suggests that the organization must undertake substantial efforts to understand and implement requisite security standards to ensure alignment with best practices and regulatory obligations. The other options represent varying degrees of compliance that do not align with the definition of "Non-Compliant". Each of those percentages indicates that some level of compliance exists, which contradicts the essence of being deemed non-compliant.

10. What is the main function of the HITRUST Common Security Framework?

A. Provide a guideline for risk assessment

B. Serve as a framework for health information security

C. Establish a set of national security standards

D. Ensure only technical compliance

The main function of the HITRUST Common Security Framework (CSF) is to serve as a comprehensive framework for health information security. This framework integrates various existing security standards, regulations, and best practices to address the need for comprehensive protection of sensitive health information. It is designed specifically to meet the unique challenges of the healthcare industry and provide a structured approach to safeguarding data. By aligning with regulations such as HIPAA, and combining various security controls, the HITRUST CSF helps organizations implement effective security programs, ensuring the confidentiality, integrity, and availability of health information. This is vital for maintaining trust and compliance in the healthcare sector, where data breaches can have significant repercussions. The other options, while relevant to the broader context of security and risk management, do not encapsulate the primary role of the framework as effectively. The HITRUST CSF goes beyond merely providing guidelines for risk assessment, establishing a set of national standards, or ensuring only technical compliance, focusing instead on a holistic approach to health information security that encompasses various aspects of data protection.

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://hitrustccsfp.examzify.com

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