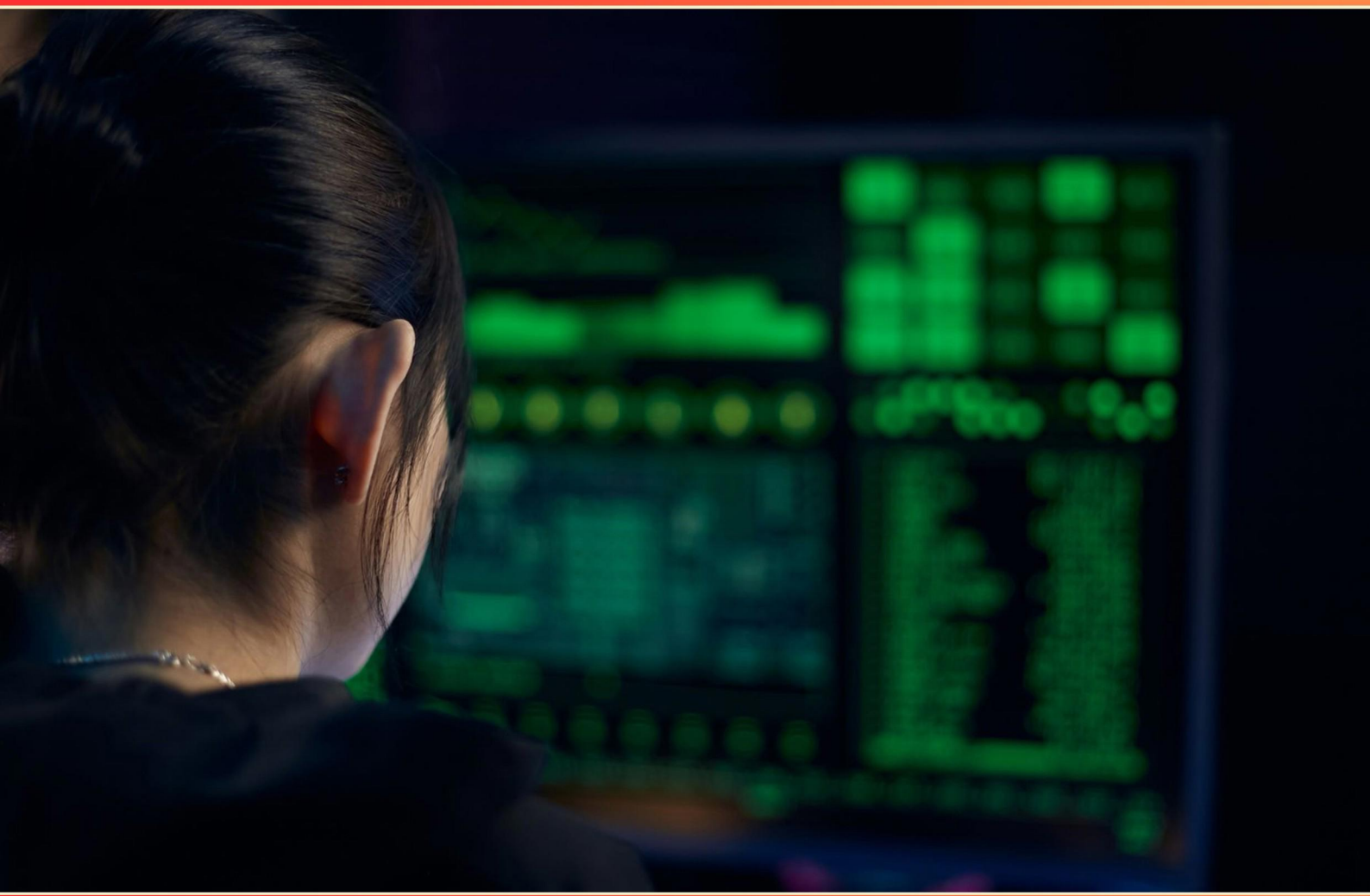
INFORMATION SYSTEMS TECHNICIAN FIRST CLASS (IT1) ADVANCEMENT PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://it1advancement.examzify.com

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

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

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. What does the Physical Layer (Layer 1) in the OSI model address?

A. Data formatting

B. Network protocols

C. Electrical, mechanical, and functional interfaces

D. Data error correction

2. Who is responsible for overseeing compliance with government IT security regulations?

A. NAVCYBERFOR

B. COMNAVCYBERFORINST 5239.1

C. DoD IA Awareness

D. IAM

3. What is the maximum time keymat marked "crypto" must be destroyed after suppression?

A. 24 hours

B. 12 hours

C. 36 hours

D. 5 days

4. What do protocols define in a network?

A. Hardware configurations

B. Methods for data storage

C. How networks establish communications and exchange info

D. Network security measures

5. Who is responsible for maintaining the appropriate operational IA posture for an organization?

A. IA Vulnerability Management

B. IAM

C. IAO

D. NAVCYBERFOR

SAMPLE

6. Which code is used within emergency response to signify a need for immediate action?

A. SECURATE

B. NC

C. Orange

D. Frequency Planning

7. Which layer ensures that data units are sent without losses or duplication?

A. Application layer

B. Transport layer

C. Network layer

D. Session layer

8. What does reverse AGC voltage do in a receiver?

A. Increases gain consistently

B. Drives amplifiers toward cutoff

C. Amplifies the received signal

D. Reduces the noise level

9. How does the amplitude of a wave relate to its energy transmission?

A. Higher amplitude means less energy

B. Higher amplitude means more energy

C. Amplitude has no effect on energy

D. Amplitude affects only frequency

10. Military communications are primarily divided into which two classes?

A. Personal and Private

B. Emergency and Non-Emergency

C. Tactical and Strategic

D. Local and Global

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does the Physical Layer (Layer 1) in the OSI model address?

A. Data formatting

B. Network protocols

C. Electrical, mechanical, and functional interfaces

D. Data error correction

The Physical Layer, which is the first layer of the OSI model, is primarily concerned with the electrical, mechanical, and functional interfaces that enable communication between devices. This layer defines the physical characteristics of the network medium used for transmission, including aspects such as voltage levels, timing of voltage changes, physical data rates, and the physical layout of the network's hardware components, such as cables and connectors. This layer serves as the foundation for the entire OSI model, facilitating the actual transmission of raw bit streams over a physical medium, such as copper wire, fiber optic cables, or wireless signals. It does not handle any higher-level functions such as data formatting or error correction, which are managed by the layers above it in the OSI model. Thus, the emphasis on electrical and mechanical parameters is key to understanding the role of the Physical Layer in network communication.

2. Who is responsible for overseeing compliance with government IT security regulations?

A. NAVCYBERFOR

B. COMNAVCYBERFORINST 5239.1

C. DoD IA Awareness

D. IAM

The responsibility for overseeing compliance with government IT security regulations primarily lies with NAVCYBERFOR, which is the U.S. Navy's command focused on cybersecurity and information assurance. NAVCYBERFOR provides guidance, policy, and oversight for the Navy's cyber operations, ensuring that all IT security measures align with federal regulations and military standards. This entity plays a crucial role in developing and enforcing cybersecurity policies across the Navy, making it the appropriate answer. By managing and auditing compliance with necessary security measures, NAVCYBERFOR helps facilitate a secure operational environment that aligns with broader governmental IT security mandates. The other options, while relevant in the context of IT security and awareness, do not have the same level of authority or responsibility. COMNAVCYBERFORINST 5239.1 is a specific instruction that outlines policy but does not oversee compliance itself. DoD IA Awareness pertains to the training and education of personnel regarding Information Assurance but does not oversee compliance directly. IAM refers to Information Assurance Managers, who implement security measures but are part of the broader structure rather than being ultimately responsible for compliance oversight.

SAMPLE

3. What is the maximum time keymat marked "crypto" must be destroyed after suppression?

A. 24 hours

B. 12 hours

C. 36 hours

D. 5 days

The correct answer, which indicates that keymat marked "crypto" must be destroyed within 12 hours after suppression, is rooted in the stringent protocols surrounding the handling of cryptographic materials. This timeframe is established to ensure that sensitive cryptographic keys do not remain vulnerable or accessible for longer than necessary, thereby maintaining the integrity and confidentiality of classified information. The requirement for the 12-hour destruction mandate stems from practices intended to mitigate risks associated with unauthorized access to cryptographic assets. Timely destruction minimises the window of opportunity for potential compromise, ensuring that once the need for the key material is eliminated, remnants cannot be exploited. A longer time allowance, such as 24 hours or 36 hours, would increase the risk of exposure, which is why the 12-hour limit is a critical standard in information security protocols regarding cryptographic key management. Always adhering to the specified destruction period for cryptographic materials is vital in safeguarding national security and maintaining trust in secure communications.

4. What do protocols define in a network?

A. Hardware configurations

B. Methods for data storage

C. How networks establish communications and exchange info

D. Network security measures

Protocols in a network are fundamental because they define the rules and conventions for communication between network devices. This includes how data is packaged, transmitted, and received across the network. Specifically, protocols govern aspects such as: - The format of the messages being sent, - The procedure for establishing connections, - Error detection and correction methods, - Data flow control, - The sequence in which different pieces of information are exchanged. By adhering to these established protocols, devices from different manufacturers can interoperate smoothly, ensuring consistent communication across diverse hardware and software environments. This is essential for creating reliable, efficient, and scalable network interactions, which is why the option focusing on how networks establish communications and exchange information is correct. The other options focus on aspects like hardware configurations or security measures, which, while important in their own right, are not central to what a protocol is designed to accomplish in a networking context.

SAMPLE

5. Who is responsible for maintaining the appropriate operational IA posture for an organization?

A. IA Vulnerability Management

B. IAM

C. IAO

D. NAVCYBERFOR

The individual responsible for maintaining the appropriate operational Information Assurance (IA) posture within an organization is the Information Assurance Officer (IAO). The IAO plays a crucial role in establishing and enforcing the organization's security policies and ensuring compliance with regulatory standards. This individual's duties often involve assessing risks, implementing security measures, and overseeing the organization's information systems to protect against threats. The IAO serves as the primary point of contact for all matters relating to information assurance and security, ensuring that security practices align with organizational goals. They are tasked with continuously evaluating the IA posture and making necessary adjustments to mitigate risks, which is essential for maintaining the integrity, confidentiality, and availability of information systems. While the other options involve important aspects of information assurance, they have distinct roles. For instance, IA Vulnerability Management pertains more specifically to identifying and managing vulnerabilities rather than overseeing the broader operational posture. The Information Assurance Manager (IAM) typically focuses on higher-level strategic initiatives and may oversee multiple IAOs rather than directly managing the operations themselves. NAVCYBERFOR primarily functions in a support and advisory capacity within the Navy's cyber operations and is not directly responsible for an individual organization's IA posture. Therefore, the clear responsibility for maintaining the operational IA posture rests with the Information Assurance Officer

6. Which code is used within emergency response to signify a need for immediate action?

A. SECURATE

B. NC

C. Orange

D. Frequency Planning

The code that is used within emergency response to signify a need for immediate action is 'NC', which stands for "No Communication." This code indicates an urgent situation that requires immediate attention, often signaling that communication has been lost or is critically limited, necessitating swift action from emergency responders. Understanding the context of emergency response codes is crucial, as they establish a clear and efficient means of communication in high-pressure situations. In scenarios where rapid decision-making and coordination are essential, using standardized codes helps ensure that all parties involved understand the urgency of the situation without ambiguity. Other terms or codes mentioned such as 'SECURATE', 'Orange', and 'Frequency Planning' do not convey immediate action in the context of emergency responsiveness in the same way that 'NC' does. For example, 'SECURATE' might refer to securing the area or situation, while 'Orange' could be related to specific preparedness levels or alerts in other contexts. 'Frequency Planning' is technical and pertains more to communication strategies rather than indicating a direct need for immediate action.

SAMPLE

7. Which layer ensures that data units are sent without losses or duplication?

A. Application layer

B. Transport layer

C. Network layer

D. Session layer

The transport layer is responsible for ensuring that data units are sent without losses or duplication. This layer manages the delivery of messages between computers and establishes a reliable communication channel. It ensures that data packets are delivered in order, without errors, and that any lost packets are retransmitted. Protocols such as Transmission Control Protocol (TCP) operate at this layer to provide end-to-end error detection and recovery mechanisms. This is crucial for applications that rely on accurate data delivery, such as web browsers and file transfer applications. In contrast, the application, network, and session layers serve different functions. The application layer is focused on providing network services directly to user applications, while the network layer is responsible for data routing and addressing but does not ensure reliable delivery. The session layer manages sessions between applications but does not handle the error recovery or data integrity that the transport layer does.

8. What does reverse AGC voltage do in a receiver?

A. Increases gain consistently

B. Drives amplifiers toward cutoff

C. Amplifies the received signal

D. Reduces the noise level

Reverse AGC (Automatic Gain Control) voltage in a receiver is primarily designed to manage the level of gain applied to the incoming signal based on its amplitude. When a strong signal is received, the reverse AGC voltage is increased, effectively driving the amplifiers toward cutoff. This action helps to prevent overload and distortion in the receiver by reducing the gain of the signal. By pushing the amplifiers toward cutoff, the receiver can maintain a more consistent output level, which is especially important in preventing strong signals from overwhelming weaker ones. This process ensures that the receiver can handle varying signal strengths without compromising the quality of the audio or data being transmitted.

9. How does the amplitude of a wave relate to its energy transmission?

A. Higher amplitude means less energy

B. Higher amplitude means more energy

C. Amplitude has no effect on energy

D. Amplitude affects only frequency

The relationship between the amplitude of a wave and its energy transmission is directly proportional. When the amplitude of a wave increases, the energy carried by that wave also increases. This is because energy in waves—such as sound or electromagnetic waves—depends on the height of the wave. A larger amplitude signifies that the wave has more energy to convey, which results in greater intensity. For instance, in sound waves, higher amplitude correlates with louder sounds, indicating more energy is being transmitted. Understanding this concept is essential, particularly in fields such as physics and engineering, where wave behavior plays a critical role in applications ranging from communication systems to audio technologies. Additionally, this relationship is foundational in various scientific disciplines, including optics and acoustics. The other options misrepresent the fundamental principles of wave dynamics, incorrectly suggesting minimal or no impact of amplitude on energy transmission.

SAMPLE

10. Military communications are primarily divided into which two classes?

A. Personal and Private

B. Emergency and Non-Emergency

C. Tactical and Strategic

D. Local and Global

The division of military communications into tactical and strategic classes is based on the purpose and scope of the communication's use. Tactical communications refer to the immediate communication needs of military units engaged in operations, focusing on the execution of specific missions or tasks. This includes real-time coordination, intelligence sharing, and command and control communications that are essential during combat or military operations. On the other hand, strategic communications involve broader planning and coordination at higher command levels, encompassing long-term objectives, policies, and overall military strategy. This type of communication is crucial for disseminating information that shapes operational readiness, resource allocation, and overall national defense strategies. Understanding the distinction between tactical and strategic communications is vital for military personnel as it dictates the type of information that is communicated, the channels used, and the urgency of the messages being sent. This framework enables effective command and control structures essential to military effectiveness.

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://it1advancement.examzify.com

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

SAMPLE