

ARMY ICTL PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR
THE FULL VERSION STUDY GUIDE

<https://armyictl.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	9
Explanations	11
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.

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

SAMPLE

- 1. Which RAID level provides mirroring for redundancy but no performance improvement?**
 - A. RAID 1
 - B. RAID 0
 - C. RAID 5
 - D. RAID 6

- 2. Which protocol is preferred for secure remote management over the network?**
 - A. Telnet
 - B. HTTP
 - C. FTP
 - D. Secure Shell

- 3. Differentiate among IaaS, PaaS, and SaaS with an Army-IT example for each.**
 - A. IaaS provides virtualized computing resources (e.g., Army-hosted infrastructure); PaaS provides a runtime environment for applications (e.g., development platform); SaaS provides ready-to-use applications (e.g., email/office apps).
 - B. IaaS provides ready-to-use applications; PaaS provides virtualized resources; SaaS provides runtime platforms.
 - C. IaaS provides a runtime environment for applications; PaaS provides ready-to-use applications; SaaS provides infrastructure resources.
 - D. IaaS, PaaS, SaaS are all the same.

- 4. Which statement accurately describes the difference between Windows Control Panel and Settings?**
 - A. The Settings app is the modern, centralized interface for configuration and updates.
 - B. The Control Panel and Settings app are identical in tools and layout.
 - C. The Control Panel provides legacy, classic tools; Settings is the modern centralized interface for configuration and updates.
 - D. The Settings app is deprecated and no longer used.

- 5. What type of attack is a Man-in-the-Middle Attack considered?**
- A. A phishing tactic.
 - B. A type of eavesdropping.
 - C. A ransomware scheme.
 - D. An authority-level hack.
- 6. Which set of terms represents the components of the CIA triad?**
- A. Integrity, Availability, Authentication
 - B. Confidentiality, Availability, Privacy
 - C. Confidentiality, Integrity, Availability
 - D. Privacy, Integrity, Availability
- 7. Which device is primarily responsible for interconnecting networks by forwarding information based on IP addresses?**
- A. Router
 - B. Switch
 - C. Hub
 - D. Bridge
- 8. Name a typical stage in an incident response lifecycle.**
- A. Eradication
 - B. Containment
 - C. Recovery
 - D. Preparation
- 9. Between SSH and Telnet, which provides encrypted remote access suitable for management?**
- A. Telnet
 - B. Secure Shell
 - C. HTTP
 - D. FTP

10. Vishing primarily relies on which communication method?

- A. Voice calls using traditional phones or VoIP.
- B. Phishing emails.
- C. SMS messages.
- D. Social media messaging.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which RAID level provides mirroring for redundancy but no performance improvement?

A. RAID 1

B. RAID 0

C. RAID 5

D. RAID 6

RAID 1 is the setup that mirrors data on a second drive, providing redundancy so you can continue if one disk fails. Because every write has to go to both drives, there isn't a real speed-up for writes, so you don't gain performance. You might see a small read improvement since reads can come from either disc, but the main benefit is fault tolerance, not speed. The other RAID levels either have no redundancy (striping) or use parity to recover data, which affects performance differently.

2. Which protocol is preferred for secure remote management over the network?

A. Telnet

B. HTTP

C. FTP

D. Secure Shell

When you need to manage devices remotely over a network, you want an encrypted, authenticated session that protects both the data you send and your credentials. Telnet transmits everything in plaintext, so passwords and commands can be read by anyone snooping the network. HTTP and FTP aren't designed for secure remote administration, and FTP in particular sends user credentials in the clear. Secure Shell, on the other hand, creates an encrypted channel for remote login and command execution, with strong authentication and data integrity. It shields commands and output from eavesdropping, tampering, and impersonation, and it also supports secure file transfer (SCP/SFTP) and features like port forwarding for protecting additional services. For these protections and capabilities, SSH is the preferred protocol for secure remote management over the network.

3. Differentiate among IaaS, PaaS, and SaaS with an Army-IT example for each.

- A. IaaS provides virtualized computing resources (e.g., Army-hosted infrastructure); PaaS provides a runtime environment for applications (e.g., development platform); SaaS provides ready-to-use applications (e.g., email/office apps).**
- B. IaaS provides ready-to-use applications; PaaS provides virtualized resources; SaaS provides runtime platforms.
- C. IaaS provides a runtime environment for applications; PaaS provides ready-to-use applications; SaaS provides infrastructure resources.
- D. IaaS, PaaS, SaaS are all the same.

Understanding what each cloud service model provides helps you see how they differ in control and responsibility. In IaaS, you rent the basic computing resources—virtual servers, storage, and networking—while you manage the operating systems and applications that run on top. An Army-IT example is hosting the Army's data center infrastructure in a virtualized form, where units provision and scale their own virtual machines as needed. In PaaS, you get a platform that includes a runtime environment and tooling to develop, deploy, and manage applications, without worrying about the underlying hardware or OS setup. An Army example would be a secure development platform that provides middleware, databases, and deployment pipelines so developers can build and release Army apps more efficiently. In SaaS, you access ready-to-use software over the internet, with the provider handling everything from the infrastructure to the application itself. An Army example is email or office productivity tools delivered through the cloud, enabling use without local installation and with centralized security controls. This combination matches the described option because it correctly assigns each service model to its typical responsibility and a representative Army-IT example. The other descriptions blur these distinctions by suggesting IaaS offers ready-made apps, PaaS offers infrastructure, or SaaS handles runtime environments, which misstates what each service level provides.

4. Which statement accurately describes the difference between Windows Control Panel and Settings?

- A. The Settings app is the modern, centralized interface for configuration and updates.
- B. The Control Panel and Settings app are identical in tools and layout.
- C. The Control Panel provides legacy, classic tools; Settings is the modern centralized interface for configuration and updates.**
- D. The Settings app is deprecated and no longer used.

Windows uses two interfaces for configuring the system: a modern, centralized Settings app and the older Control Panel that hosts legacy tools. The Settings app is designed to be the main place for most configuration tasks and for managing updates, with a streamlined, category-based layout that's consistent across Windows versions. The Control Panel, meanwhile, contains traditional administration tools that originated in earlier Windows releases and haven't been fully migrated to Settings. Because of this distinction, the statement that the Control Panel provides legacy, classic tools while Settings serves as the modern centralized interface for configuration and updates is accurate. It's not true that the two are identical in tools and layout, and Settings isn't deprecated.

5. What type of attack is a Man-in-the-Middle Attack considered?

- A. A phishing tactic.
- B. A type of eavesdropping.**
- C. A ransomware scheme.
- D. An authority-level hack.

Interception of communications between two parties—seeing and potentially altering data as it travels—is what a Man-in-the-Middle attack centers on. This makes it a form of eavesdropping, since the attacker can listen to and read the exchanged information. Phishing relies on tricking people into revealing credentials or data rather than quietly watching a live connection. Ransomware encrypts files for ransom, not intercepting traffic. An authority-level hack isn't a standard category for this kind of activity. Defenses include end-to-end encryption, proper certificate validation, and secure network practices to prevent attackers from positioning themselves between communicating endpoints.

6. Which set of terms represents the components of the CIA triad?

- A. Integrity, Availability, Authentication
- B. Confidentiality, Availability, Privacy
- C. Confidentiality, Integrity, Availability**
- D. Privacy, Integrity, Availability

This set aligns with the CIA triad, the fundamental goals of information security: keeping information confidential from unauthorized parties, ensuring it remains accurate and unaltered, and making sure authorized users can access it when needed. Confidentiality protects who can see the data, integrity guards that data isn't tampered with, and availability ensures access is available to those who are authorized. Authentication and privacy are important concepts in security, but they aren't the three core components of the CIA triad. Authentication is about verifying identity, not a triad component, and privacy concerns how data is collected and used, which is related but separate from the triad's three protections. Therefore, Confidentiality, Integrity, and Availability best represent the CIA triad.

7. Which device is primarily responsible for interconnecting networks by forwarding information based on IP addresses?

- A. Router**
- B. Switch
- C. Hub
- D. Bridge

Routing between networks relies on a device that examines the IP header and uses a routing table to forward packets toward their destination. This happens at the network layer, so the device that connects multiple IP networks (subnets) and decides the next hop based on the destination IP address is a router. It can link different networks, including LANs and WANs, and can use routing protocols to learn the best paths. Switches, by contrast, operate mainly at the data link layer and forward frames using MAC addresses within the same network, which is why they're ideal for local device connectivity but not for inter-network routing. Hubs simply repeat all signals to every port without any forwarding intelligence. Bridges connect two LAN segments but still make decisions based on MAC addresses, not IP addresses, so they don't route between different networks. So, the device that interconnects networks by forwarding information based on IP addresses is the router.

8. Name a typical stage in an incident response lifecycle.

- A. Eradication
- B. Containment**
- C. Recovery
- D. Preparation

Containment is a typical stage in the incident response lifecycle because, once an incident is detected, the immediate priority is to stop the spread and minimize damage. Containment actions aim to isolate affected systems, block attacker access, and segment networks so the threat cannot move laterally or exfiltrate data. This pause in activity buys time for investigation and planning, helping preserve evidence and prevent further impact while the team works out the full scope of the breach. After containment, efforts shift to eradication (removing the threat and artifacts) and recovery (bringing systems back online and verifying they're clean), with preparation (planning and preventative controls) happening beforehand to reduce future incidents.

9. Between SSH and Telnet, which provides encrypted remote access suitable for management?

- A. Telnet
- B. Secure Shell
- C. HTTP
- D. FTP**

Encrypted remote management relies on a secure channel that protects both credentials and commands as they travel across the network. Secure Shell provides exactly that by encrypting the entire session, so login details and subsequent actions cannot be easily intercepted or tampered with. Telnet, in contrast, transmits data in plaintext, exposing passwords and commands to anyone who can sniff the network. HTTP is for web traffic, not interactive remote management, and FTP is for file transfer rather than secure remote command access (even though secure variants exist, they serve different purposes). So for encrypted remote access suitable for management, Secure Shell is the correct choice.

10. Vishing primarily relies on which communication method?

- A. Voice calls using traditional phones or VoIP.**
- B. Phishing emails.
- C. SMS messages.
- D. Social media messaging.

Vishing relies on using voice channels to trick people. In vishing, the attacker makes a phone call—whether on a traditional landline or over VoIP—and impersonates a trusted entity to coax the target into revealing sensitive information or performing actions. The essence is the spoken, real-time interaction that persuades the victim, often leveraging urgency or fear. That's why voice calls using traditional phones or VoIP are the best fit. Phishing emails, SMS messages, and social media messages involve other communication channels (email, text, or chat) and are associated with different techniques like phishing, smishing, or social engineering via messaging, not the voice-based tactic defined by vishing.

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://armyictl.examzify.com>

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

SAMPLE