

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	8
Explanations	10
Next Steps	15

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. What is the purpose of SPF, DKIM, and DMARC in email security?**
 - A. They are used to verify the authenticity of emails and prevent spoofing.
 - B. They are used to filter content based on keywords.
 - C. They are used to encrypt emails end-to-end.
 - D. They replace antivirus in endpoint security.
- 2. What are clients in relation to a server?**
 - A. Programs that run only on the server
 - B. Other system entities that make requests to the server
 - C. A storage location managed by the server
 - D. Users who access the server through a GUI
- 3. How is data typically protected in transit on the Internet?**
 - A. Plain text transmission
 - B. Network isolation via VLANs
 - C. Token-based authentication only
 - D. Encryption with TLS/SSL
- 4. If you plan for a subnet requiring at least 200 host addresses, would a 192.168.0.0/24 subnet meet the requirement, and why?**
 - A. No, a /24 supports only 128 host addresses.
 - B. Yes, a /24 supports up to 200 host addresses.
 - C. Yes, a /24 supports up to 500 host addresses.
 - D. Yes, a /24 supports up to 254 host addresses, which exceeds 200.
- 5. Why is patch management important, and what is a typical patch cycle?**
 - A. A cycle that includes vendor negotiations.
 - B. Patches fix security vulnerabilities; cycle includes inventory, assessment, testing, deployment, and verification.
 - C. A cycle focused only on deployment.
 - D. A cycle that excludes verification.

6. What is RAM, and why is it important for system performance?

- A. RAM is volatile primary storage that the CPU uses for active processes; more RAM reduces paging to disk and improves performance.
- B. RAM is non-volatile storage used for long-term data; more RAM slows down performance.
- C. RAM stores graphics memory only; memory size has no impact on performance.
- D. RAM is used solely for caching network data; does not affect program execution.

7. What is a disaster recovery plan, and what are its key components?

- A. A plan to upgrade hardware on a schedule.
- B. A documented plan to recover IT services after a disruption; components include roles, contact lists, procedures, backups, testing, and maintenance.
- C. A plan for training new employees in marketing.
- D. A budget plan for IT projects.

8. Which cloud service model delivers software applications over the internet as a service?

- A. IaaS
- B. PaaS
- C. SaaS
- D. DaaS

9. What does DNS stand for?

- A. Digital Network Service.
- B. Domain Name System.
- C. Data Name Server.
- D. Dynamic Name System.

10. Which commands display IP configuration on Windows and on Linux?

- A. Windows: ipconfig; Linux: ifconfig or ip
- B. Windows: ifconfig; Linux: ipconfig
- C. Windows: tracert; Linux: traceroute
- D. Windows: netstat; Linux: netstat

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the purpose of SPF, DKIM, and DMARC in email security?

- A. They are used to verify the authenticity of emails and prevent spoofing.
- B. They are used to filter content based on keywords.
- C. They are used to encrypt emails end-to-end.
- D. They replace antivirus in endpoint security.

Authenticity of the sender and integrity of the message are what SPF, DKIM, and DMARC are designed to protect. SPF checks that the sending server is authorized to send for the domain by publishing allowed mail servers in a DNS record; when a recipient gets the mail, it compares the sending server's IP against that record and can reject or flag messages from unapproved servers. DKIM adds a cryptographic signature to the message that the recipient can verify with the domain's public key published in DNS, ensuring the email really came from that domain and hasn't been altered in transit. DMARC ties SPF and DKIM results to the domain in the From header and instructs how to handle messages that fail, plus provides reporting to domain owners. Together, they help prevent spoofing and improve trust in email. Other options aren't accurate: keyword-based filtering is a separate spam-filter function, end-to-end encryption is a different capability (like S/MIME or PGP), and these standards don't replace antivirus in endpoint security.

2. What are clients in relation to a server?

- A. Programs that run only on the server
- B. Other system entities that make requests to the server
- C. A storage location managed by the server
- D. Users who access the server through a GUI

In client-server communication, the key idea is that the client is the entity that asks for services from a server. These clients can be software programs, processes, or devices that initiate a request over the network to obtain resources or perform actions, and then wait for the server's response. This definition is broader than just human users—any program or device that makes requests qualifies as a client. Why this fits best: the server provides resources or services, and the client is the party that calls upon those services. The other options don't capture that requesting role. A storage location managed by the server is just a resource, not the requester. Users who access through a GUI describe people, not the requesting entity in the network sense. Programs that run only on the server describe server-side components, not the clients that issue requests.

3. How is data typically protected in transit on the Internet?

- A. Plain text transmission
- B. Network isolation via VLANs
- C. Token-based authentication only
- D. Encryption with TLS/SSL

Data protection in transit on the Internet is achieved by encrypting the data as it moves between endpoints, with TLS/SSL serving as the standard method. TLS provides confidentiality, integrity, and authentication for web traffic and other network communications. During a TLS handshake, the client and server verify each other's identities with certificates and agree on a shared session key. That key is used to encrypt the actual data with a fast symmetric cipher, so anyone who intercepts the packets cannot read the contents. The process also protects against tampering, as the data includes integrity checks that reveal if it has been altered. Modern TLS setups often include forward secrecy, ensuring that even if a server's private key is compromised later, past conversations stay protected because new session keys are generated for each session. In everyday use, this is why websites use HTTPS to secure browser-to-server traffic. Plain text transmission offers no confidentiality, VLANs only isolate segments within a network and don't protect data as it traverses the global Internet, and token-based authentication deals with access control rather than encrypting the data in transit. Encryption with TLS/SSL directly addresses protecting data as it travels over the Internet.

4. If you plan for a subnet requiring at least 200 host addresses, would a 192.168.0.0/24 subnet meet the requirement, and why?

- A. No, a /24 supports only 128 host addresses.
- B. Yes, a /24 supports up to 200 host addresses.
- C. Yes, a /24 supports up to 500 host addresses.
- D. Yes, a /24 supports up to 254 host addresses, which exceeds 200.**

A subnet's size determines how many hosts it can support. For a /24, there are $2^{(32-24)} = 256$ total addresses. Two addresses are reserved for the network and broadcast, leaving 254 usable host addresses. Since you need at least 200, a /24 provides enough addresses because $254 > 200$. The other options either understate the capacity (128 usable addresses) or overstate it (500), while a /24 simply cannot offer 500 usable hosts. Therefore, 192.168.0.0/24 meets the requirement.

5. Why is patch management important, and what is a typical patch cycle?

- A. A cycle that includes vendor negotiations.
- B. Patches fix security vulnerabilities; cycle includes inventory, assessment, testing, deployment, and verification.
- C. A cycle focused only on deployment.
- D. A cycle that excludes verification.**

Patch management reduces risk by addressing known vulnerabilities through updates. A typical patch cycle starts with inventory to identify what hardware and software exist and need updates, then assessment to determine urgency and potential impact, followed by testing to ensure patches don't disrupt critical systems, then deployment to apply the patches, and finally verification to confirm that patches are installed correctly and systems are functioning as expected. This sequence matters because you can't rely on deployment alone—you must know what needs patching, ensure compatibility, confirm successful installation, and verify ongoing security. Vendor negotiations aren't part of the cycle, focusing only on deployment misses planning and risk checks, and a cycle that excludes verification would leave you unsure whether patches actually took effect or if issues were introduced.

6. What is RAM, and why is it important for system performance?

- A. RAM is volatile primary storage that the CPU uses for active processes; more RAM reduces paging to disk and improves performance.**
- B. RAM is non-volatile storage used for long-term data; more RAM slows down performance.
- C. RAM stores graphics memory only; memory size has no impact on performance.
- D. RAM is used solely for caching network data; does not affect program execution.

RAM is the fast, volatile memory that holds the data and instructions the CPU is actively working with. Because it's much quicker to access than storage on a hard drive or SSD, keeping active programs and their data in RAM lets the CPU fetch what it needs quickly, which makes programs load faster and keeps the system responsive. When there isn't enough RAM, the system starts moving data that isn't immediately needed out to a swap or paging file on slower storage. This swapping slows things down dramatically because the CPU has to read and write to disk instead of RAM, leading to noticeable performance drops. So, more RAM lets more of the working set of programs reside in fast memory, reducing or eliminating the need for slow paging and improving overall performance. RAM isn't non-volatile long-term storage, it isn't limited to graphics data, and it does impact how quickly programs run, not just network caching.

7. What is a disaster recovery plan, and what are its key components?

- A. A plan to upgrade hardware on a schedule.
- B. A documented plan to recover IT services after a disruption; components include roles, contact lists, procedures, backups, testing, and maintenance.**
- C. A plan for training new employees in marketing.
- D. A budget plan for IT projects.

A disaster recovery plan is a documented set of procedures for restoring IT services after a disruption. It guides who does what, how to contact the right people, and the exact steps to recover systems and data, often including how backups are used to bring services back online. Key parts include: - Roles and responsibilities so the right people know who makes decisions and who executes tasks. - Contact lists for internal staff and external vendors or partners needed during a recovery. - Procedures that lay out step-by-step actions to recover critical services, including any failover or restoration processes. - Backups and data restoration procedures to ensure data can be recovered and systems can be brought back to a known good state. - Testing to practice the recovery, verify that steps work, and identify gaps to fix. - Maintenance to keep the plan current with changes in technology, personnel, and suppliers. Other options describe different kinds of plans (such as hardware upgrade schedules, marketing training, or IT budgeting) and don't address how to recover IT services after a disruption.

8. Which cloud service model delivers software applications over the internet as a service?

- A. IaaS
- B. PaaS
- C. SaaS**
- D. DaaS

The main idea tested here is how cloud services deliver software. The model that provides software applications over the internet as a service is Software as a Service, or SaaS. With SaaS, the provider hosts the application, handles maintenance, updates, and security, and you access the software through a web browser or thin client. You don't install or manage the underlying system yourself, and billing is usually on a subscription basis, making it quick to use and easy to scale. This differs from IaaS, which gives you core computing resources (like virtual machines and storage) that you manage yourself; and PaaS, which offers a platform to develop and run your own apps without worrying about the underlying infrastructure. DaaS isn't focused on delivering traditional software applications as a service.

9. What does DNS stand for?

- A. Digital Network Service.
- B. Domain Name System.**
- C. Data Name Server.
- D. Dynamic Name System.

DNS is the system that lets people use easy-to-remember addresses like example.com instead of long numerical IP addresses. It stands for Domain Name System because it's the global, hierarchical setup that translates domain names into the IP addresses computers use to locate resources on the network. When you access a domain, your device asks a DNS resolver, which may check its cache and then query a chain of servers (root, top-level domain, and authoritative name servers) until it returns the correct IP address so the connection can be made. The other options don't fit what this system does: Digital Network Service isn't the established term for translating names to numbers, Data Name Server isn't the standard name for the whole system, and Dynamic Name System isn't the recognized name and could imply a different concept.

10. Which commands display IP configuration on Windows and on Linux?

A. Windows: ipconfig; Linux: ifconfig or ip

B. Windows: ifconfig; Linux: ipconfig

C. Windows: tracert; Linux: traceroute

D. Windows: netstat; Linux: netstat

This question tests knowing which commands show IP configuration on each platform. On Windows, ipconfig reveals the system's IP address, subnet mask, default gateway, and DNS servers. On Linux, you can use ifconfig to view similar details, though the modern tool is ip (from iproute2), with ip addr (or ip a) giving the interface addresses. So pairing Windows with ipconfig and Linux with either ifconfig or ip captures how to display IP configuration across both systems. The other options mix in commands that serve different purposes, like tracing routes to destinations or showing active connections, which don't display the local IP configuration.

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://armyictl.examzify.com>

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

SAMPLE