Information Technology Specialist (MOS 25B) Practice Test (Sample)

Study Guide

Table of Contents

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. Don't worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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

1. **What is the main focus of the principle of least privilege?**

    A. Maximizing user access for productivity

    B. Providing the highest security clearance to all users

    C. Minimizing access rights for users based on their job functions

    D. Educating users on security practices

2. **Which device allows users to tap and pay for their purchases?**

    A. Chip card reader

    B. Near-Field Communication (NFC) device

    C. Magnetic stripe reader

    D. Contactless payment terminal

3. **What best describes a SQL injection attack?**

    A. A preventive measure for web applications

    B. A malicious technique to execute unauthorized SQL commands

    C. A method to optimize database queries

    D. A strategy for securing user permissions

4. **What is one active cooling solution for a PC?**

    A. Replacing thermal paste

    B. Add an additional case fan

    C. Improving airflow

    D. Cleaning the dust from components

5. **What is used as permanent storage for data in a computer system?**

    A. RAM

    B. SSD

    C. Hard Drive

    D. Cache Memory

6. **How can employee training enhance IT security?**

   A. By teaching new software skills

   B. By making employees aware of security threats

   C. By improving physical security measures

   D. By reducing IT-related costs

7. **What is malware?**

   A. Software to improve system performance

   B. Malicious software designed to harm computers

   C. Software used to manage network traffic

   D. Programs designed for user convenience

8. **What is a possible solution to the high failure rate of hard drives in a vibration-prone environment?**

   A. Install a larger HDD

   B. Use an external drive

   C. Install an SSD drive in each computer

   D. Use RAID configuration

9. **What should a technician check to determine if an additional hard drive can be added to an older computer?**

   A. Available USB port

   B. Available PATA/SATA connection

   C. Available PCI slot

   D. Available RAM slot

10. **Which type of memory is primarily used as cache memory?**

   A. DRAM

   B. SRAM

   C. EEPROM

   D. NVM

Answers

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

Explanations

1. What is the main focus of the principle of least privilege?

A. Maximizing user access for productivity

B. Providing the highest security clearance to all users

C. Minimizing access rights for users based on their job functions

D. Educating users on security practices

The principle of least privilege emphasizes that users should have the minimum level of access—or permissions—necessary to perform their job functions effectively. This approach helps to enhance security by limiting the potential damage that can occur from accidental or malicious actions. By restricting access rights, organizations can mitigate risks associated with unauthorized access to sensitive data and systems. It ensures that users cannot access information or perform actions that are outside the scope of their responsibilities, thereby reducing vulnerabilities and making it easier to manage and control security within the environment.   In contrast, maximizing user access could lead to increased risks and potential breaches, while providing the highest security clearance indiscriminately can expose critical resources to unnecessary threats. Educating users on security practices is important, but it does not directly correlate with access rights and is not the main focus of the principle of least privilege. Therefore, minimizing access rights tailored to job functions stands out as the most relevant focus for security best practices.

2. Which device allows users to tap and pay for their purchases?

A. Chip card reader

B. Near-Field Communication (NFC) device

C. Magnetic stripe reader

D. Contactless payment terminal

The correct answer highlights the role of Near-Field Communication (NFC) technology in facilitating tap-and-pay transactions. NFC is a wireless communication standard that allows devices, such as smartphones or contactless cards, to exchange data over very short distances, typically a few centimeters. This functionality is widely utilized in various payment systems, enabling users to make secure transactions simply by tapping their NFC-enabled device near a compatible terminal. While chip card readers and contactless payment terminals also support similar payment processes, NFC stands out in the context of mobile payments, where customers can use their smartphones or smartwatches to complete transactions. Magnetic stripe readers do not enable contactless payments; instead, they require physical swipes of cards with magnetic stripes. Understanding NFC and its applications in mobile payments is essential for anyone engaged in the field of information technology and modern transaction systems.

3. What best describes a SQL injection attack?

A. A preventive measure for web applications

B. A malicious technique to execute unauthorized SQL commands

C. A method to optimize database queries

D. A strategy for securing user permissions

A SQL injection attack is defined as a malicious technique used to execute unauthorized SQL commands. This type of attack involves inserting or "injecting" malicious SQL code into a query through user input fields that are not properly sanitized. The attacker can manipulate the SQL statements that the application sends to the database, potentially allowing them to gain unauthorized access to sensitive data, alter database content, or even execute administrative operations on the database.   Understanding this concept is crucial for anyone involved in database management or web application development because it highlights the importance of implementing security measures, such as input validation and parameterized queries, to protect against such vulnerabilities.

4. What is one active cooling solution for a PC?

A. Replacing thermal paste

B. Add an additional case fan

C. Improving airflow

D. Cleaning the dust from components

Adding an additional case fan is an active cooling solution because it involves using a powered device to enhance the cooling capability of a computer system. Case fans improve air circulation by moving air in or out of the case, helping to dissipate heat generated by the internal components, such as the CPU and GPU. This active movement of air lowers temperatures more effectively than passive solutions, which simply rely on the natural convection of air. In contrast, replacing thermal paste, improving airflow, and cleaning dust from components primarily address the efficiency of existing cooling methods rather than adding new active cooling elements. While these aspects are crucial for maintaining optimal performance and heat management, they do not constitute active cooling solutions as they do not directly increase the system's cooling capacity through the introduction of additional powered components.

5. What is used as permanent storage for data in a computer system?

A. RAM

B. SSD

C. Hard Drive

D. Cache Memory

The correct choice, which is the hard drive, serves as a crucial component for permanent storage of data within a computer system. Unlike volatile memory types, such as RAM and cache memory, which lose their stored information when the system is powered off, the hard drive maintains data persistently over time.   The hard drive is capable of storing everything from the operating system and applications to personal files and multimedia, ensuring that the data remains intact until it is intentionally deleted or modified. This permanence is essential for users and systems that rely on stable access to their information. Moreover, while solid-state drives (SSDs) can also provide permanent storage and are becoming increasingly popular due to their speed and reliability, the hard drive remains a traditional and widely used solution for data storage, especially in bulk data environments. It's also important to note that cache memory and RAM are designed for different functions, mainly for temporary data access and processing speed, rather than permanent storage.

6. How can employee training enhance IT security?

A. By teaching new software skills

B. By making employees aware of security threats

C. By improving physical security measures

D. By reducing IT-related costs

Employee training can significantly enhance IT security by making employees aware of security threats. When individuals are informed about potential cyber threats, such as phishing attacks, malware, social engineering tactics, and other vulnerabilities, they become more vigilant and can recognize suspicious activities. This awareness is crucial because human error is often a major factor in security breaches.   Training programs can equip employees with the skills needed to identify and respond to threats effectively. For instance, they learn to scrutinize emails for phishing attempts, understand the importance of secure password management, and know the protocols for reporting suspicious incidents. The goal is to create a culture of security within the organization, where each employee feels responsible for protecting not only their own data but the organization's information as a whole.   In contrast, while new software skills may be beneficial to performance and productivity, they do not directly address the issue of security. Improvements in physical security measures and reducing IT-related costs, while important aspects of overall IT management, do not focus on enhancing the awareness and responsiveness of employees in relation to security threats. Thus, the training that raises awareness of security threats directly contributes to a more secure IT environment.

7. What is malware?

A. Software to improve system performance

B. Malicious software designed to harm computers

C. Software used to manage network traffic

D. Programs designed for user convenience

Malware is defined as malicious software that is specifically created to harm, exploit, or otherwise compromise the operation of computers, networks, or other devices. This can include a wide variety of harmful programs, such as viruses, worms, trojan horses, ransomware, and spyware. The intent behind malware is often to steal sensitive information, disrupt services, or gain unauthorized access to systems. In contrast, software designed to improve system performance serves legitimate purposes, enhancing user experiences and optimizing computer functions. Similarly, software that manages network traffic is used to improve the flow of data across networks, while programs designed for user convenience aim to simplify tasks and enhance usability. These options focus on benign or beneficial functions, thus distinguishing them significantly from the harmful nature of malware.

8. What is a possible solution to the high failure rate of hard drives in a vibration-prone environment?

A. Install a larger HDD

B. Use an external drive

C. Install an SSD drive in each computer

D. Use RAID configuration

Using an SSD (Solid State Drive) in each computer offers significant advantages in vibration-prone environments compared to traditional HDDs (Hard Disk Drives). Unlike HDDs, which have moving mechanical parts such as platters and read/write heads, SSDs rely on flash memory to store data. This absence of moving components makes SSDs more resistant to physical shocks and vibrations, reducing the likelihood of data loss or drive failure in unstable environments. Moreover, SSDs tend to have faster data access and transfer speeds, which can enhance overall system performance. While using an external drive or configuring RAID can provide some level of data protection and redundancy, those solutions do not fundamentally address the issue of vulnerability to vibration. Similarly, simply installing a larger HDD does not mitigate the risk associated with mechanical failure in such conditions. Therefore, choosing SSDs directly addresses the root cause of the problem, making it an effective solution to the high failure rates associated with HDDs in vibration-prone settings.

9. What should a technician check to determine if an additional hard drive can be added to an older computer?

A. Available USB port

B. Available PATA/SATA connection

C. Available PCI slot

D. Available RAM slot

A technician should check for an available PATA/SATA connection when determining if an additional hard drive can be added to an older computer because this connection is necessary for interfacing the hard drive with the motherboard. PATA (Parallel ATA) and SATA (Serial ATA) are types of interfaces used for connecting storage devices, such as hard drives, to a computer. If a PATA/SATA connection is available, this indicates that there is a way for the new hard drive to communicate with the system. Additionally, considering the older nature of the computer, limitations on the number of connections may exist, making it critical to verify that appropriate interfaces are free for use with the additional hard drive. Checking the availability of installation space and power supply is also important, but those aspects are secondary to confirming the presence of the necessary data connection. Looking at the other options, an available USB port is typically used for peripherals and external storage rather than internal hard drives. An available PCI slot is intended for expansion cards, not for storage devices. Available RAM slots pertain to memory upgrades rather than hard drive installations, hence they are not relevant to adding a hard drive. Therefore, the PATA/SATA connection serves as the crucial factor for adding an internal storage device.

10. Which type of memory is primarily used as cache memory?

A. DRAM

B. SRAM

C. EEPROM

D. NVM

SRAM, or Static Random-Access Memory, is primarily used as cache memory due to its speed and efficiency. It is designed to be faster than other types of memory, particularly Dynamic Random-Access Memory (DRAM), which is used for main memory but is slower in operation. The functionality of SRAM comes from the way it stores data. Unlike DRAM, which needs to be refreshed thousands of times per second to maintain data integrity, SRAM retains data as long as power is supplied without the need for refreshing. This characteristic allows SRAM to offer quicker access times, making it ideal for caching purposes where speed is essential. Furthermore, cache memory, which acts as a buffer between the CPU and main memory, requires a type of memory that can operate at high speeds to ensure that the processor has immediate access to frequently used data. The speed of SRAM allows CPUs to access data more rapidly, thus enhancing overall system performance. Other types of memory, such as EEPROM and NVM, serve different purposes and are not as suitable for cache applications due to their slower access speeds and complexity in operation compared to SRAM.

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://itspecialistmos25b.examzify.com

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