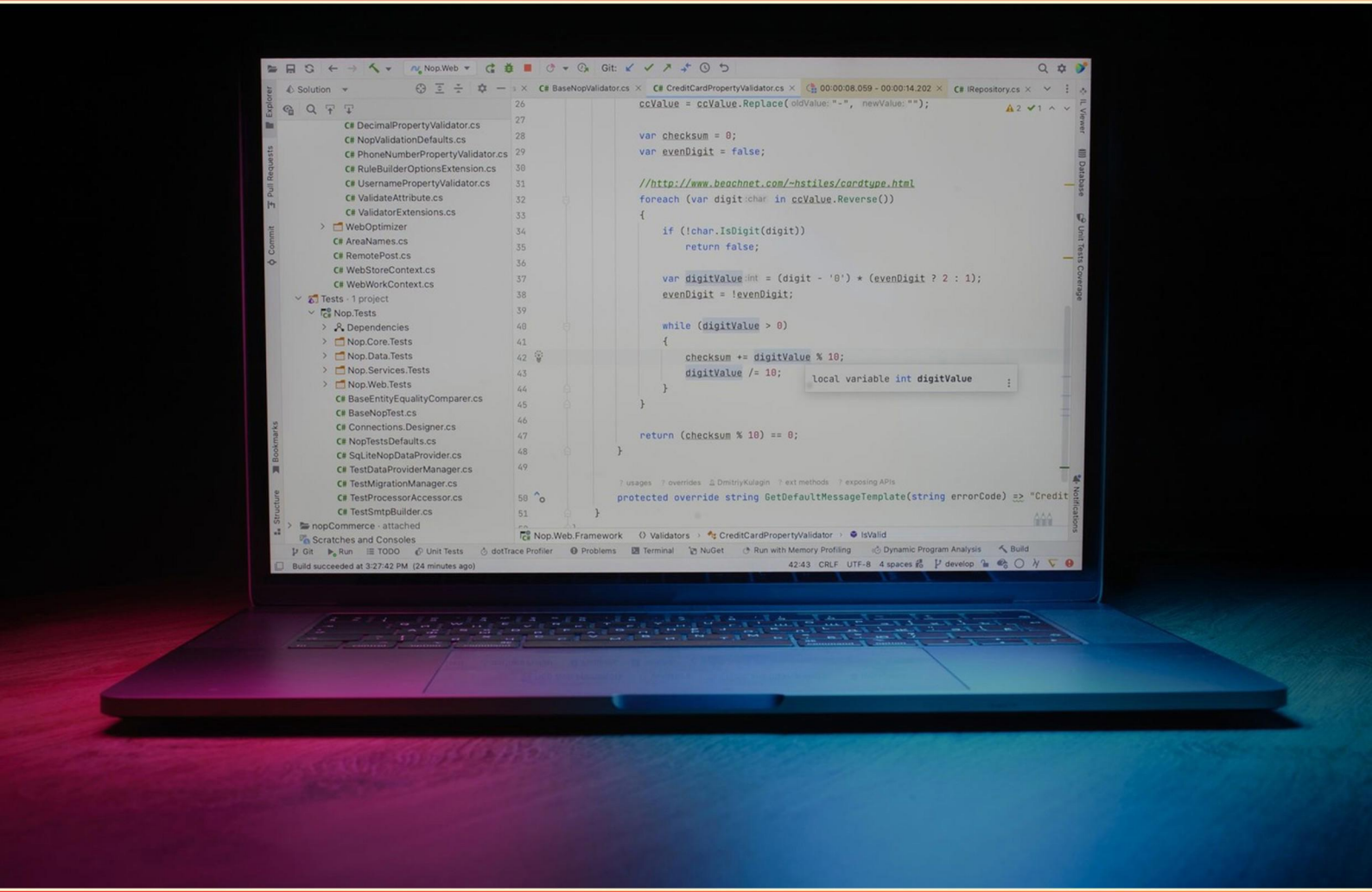
# USER ACCOUNT MANAGEMENT 25B PRACTICE TEST (SAMPLE)

## STUDY GUIDE



## SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

**VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE**

https://useracctmgmt25b.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. Phishing emails often aim to obtain what from users?**

A. Usernames and passwords

B. Network configurations

C. Physical addresses

D. Company policies

**2. What outcome is expected from adhering to a user account policy?**

A. Increased risk of unauthorized access

B. Improved employee understanding of account security

C. Less accountability among staff members

D. Time wasted on extensive training sessions

**3. Which environment involves deleting email mailboxes at the Defense Enterprise Email System?**

A. Tactical environment

B. Field environment

C. Garrison

D. Remote access environment

**4. How can User Account Management help prevent unauthorized access?**

A. By randomly assigning account passwords

B. By ensuring robust account creation practices

C. By outsourcing account management

D. By eliminating the need for passwords

**5. What is a key function of user de-provisioning?**

A. To enhance user permissions

B. To track user activity

C. To remove accounts that are no longer needed

D. To create new user accounts

**6. What does an identity management system ensure?**

A. Only authorized individuals have access to administrative functions

B. Users have access to all resources at all times

C. The right individuals have access to the right resources for the right reasons

D. All users can reset their own passwords without restrictions

SAMPLE

**7. Which is a benefit of using account lockout policies?**

A. It allows users to reset passwords easily

B. It prevents repeated login attempts from attackers

C. It provides immediate access to all users

D. It reduces the number of accounts

**8. How does a user account differ from a group account?**

A. A user account is for individuals, while a group account manages multiple users

B. A user account is temporary, while a group account is permanent

C. A user account can have unlimited permissions; a group account cannot

D. A user account is managed by IT, while a group account is user-driven

**9. In Linux, which file contains user account information?**

A. /etc/usermap

B. /etc/userinfo

C. /etc/passwd

D. /etc/accounts

**10. What aspect of password management does a password manager improve?**

A. It makes passwords easier to guess

B. It allows sharing passwords between multiple users

C. It promotes strong and unique passwords for different accounts

D. It encourages the use of simple passwords

SAMPLE

# Answers

SAMPLE

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

SAMPLE

# Explanations

SAMPLE

## 1. Phishing emails often aim to obtain what from users?

A. Usernames and passwords

B. Network configurations

C. Physical addresses

D. Company policies

*Phishing emails are specifically designed to deceive users into disclosing sensitive information, primarily their usernames and passwords. These emails typically masquerade as legitimate communication from reputable sources, such as banks, online services, or even familiar contacts, prompting users to provide their login credentials through a fraudulent webpage or form. This method is highly effective because it exploits the trust users have in known institutions. Obtaining usernames and passwords enables attackers to gain unauthorized access to personal accounts, whether it's for financial purposes, information theft, or even further infiltration into organizational networks. Since usernames and passwords are the primary keys to user accounts, their acquisition is the main goal of phishing attacks, making this the correct answer. While network configurations, physical addresses, and company policies might be of interest in certain security contexts, they are not the primary focus of phishing schemes, which concentrate on the immediate capture of login credentials.*

## 2. What outcome is expected from adhering to a user account policy?

A. Increased risk of unauthorized access

B. Improved employee understanding of account security

C. Less accountability among staff members

D. Time wasted on extensive training sessions

*Adhering to a user account policy is designed to enhance security practices within an organization, leading to an improved understanding of account security among employees. When a user account policy is implemented, it typically includes guidelines on creating strong passwords, understanding the importance of two-factor authentication, and recognizing potential phishing attempts. This structured approach reinforces the significance of security protocols among employees, fostering a culture of vigilance and individual responsibility regarding their accounts. As employees become more knowledgeable about the security measures in place and the rationale behind them, they are likely to take these guidelines seriously. This understanding helps reduce the risk of security breaches caused by negligent behavior, such as weak passwords or poor security practices. The other options do not align with the intended outcome of a user account policy. A reduction in accountability or increased risks of unauthorized access would undermine the primary goal of establishing such a policy. Time spent on training, while necessary for instilling these practices, should be viewed not as wasted time but as a crucial investment in protecting the organization's data and accounts.*

SAMPLE

## 3. Which environment involves deleting email mailboxes at the Defense Enterprise Email System?

A. Tactical environment

B. Field environment

C. Garrison

D. Remote access environment

*The correct choice pertains to the garrison environment, which is characterized by a more stable and permanent setup compared to others. In garrison environments, management tasks such as deleting email mailboxes in the Defense Enterprise Email System are conducted regularly as part of administrative duties. This includes maintaining user accounts, managing resources, and enforcing security policies, all of which are essential in supporting the operational readiness of the organization. The distinction of the garrison environment comes from its structure, where personnel are more frequently stationed in a fixed location, allowing for systematic management of resources, including email services. Other environments, such as tactical or field environments, may focus on immediate operational needs and response capabilities, which typically wouldn't prioritize routine mailbox deletions as part of their operational focus. The remote access environment is also dedicated to allowing users to connect to resources from outside their typical work environment, often emphasizing security and accessibility over mailbox management. Therefore, the process of deleting email mailboxes aligns with the defined operational procedures in a garrison setting, making it the correct answer.*

## 4. How can User Account Management help prevent unauthorized access?

A. By randomly assigning account passwords

B. By ensuring robust account creation practices

C. By outsourcing account management

D. By eliminating the need for passwords

*User Account Management plays a crucial role in preventing unauthorized access by ensuring robust account creation practices. This involves implementing policies and procedures that govern how user accounts are created, managed, and maintained. A well-structured account creation process can include several key elements, such as requiring strong, complex passwords, verifying users' identities through multi-factor authentication methods, and setting appropriate permissions based on the user's role in the organization. By focusing on strong protocols during account creation, organizations reduce the likelihood of accounts being compromised. For example, requiring users to create passwords that include a mix of letters, numbers, and special characters makes it harder for unauthorized individuals to guess passwords. Additionally, defining user roles helps ensure that individuals only have access to the information and systems necessary for their job, further minimizing risks. In contrast, simply assigning passwords randomly lacks the foresight needed to create a secure environment, while outsourcing account management might not guarantee that stringent practices are followed. The idea of eliminating the need for passwords altogether could create vulnerabilities, as it would rely entirely on alternative authentication methods, which may not always be as secure as properly managed passwords. Therefore, robust account creation practices form the foundation of effective User Account Management and are essential for safeguarding access to sensitive information.*

SAMPLE

## 5. What is a key function of user de-provisioning?

A. To enhance user permissions

B. To track user activity

C. To remove accounts that are no longer needed

D. To create new user accounts

*User de-provisioning primarily involves the process of removing user accounts that are no longer needed. This is critical for several reasons, including maintaining security and compliance within an organization. When an employee leaves or no longer requires access to certain resources, their user account must be deactivated or deleted to ensure that they cannot access sensitive information or systems. This helps prevent unauthorized access and potential security breaches, thereby safeguarding the organization's data and resources. Additionally, de-provisioning is part of a broader user lifecycle management process, which includes creating user accounts, managing permissions, and periodically reviewing access rights. The importance of proper de-provisioning cannot be overstated, as it is essential for effective access control and overall data protection within an organization.*

## 6. What does an identity management system ensure?

A. Only authorized individuals have access to administrative functions

B. Users have access to all resources at all times

C. The right individuals have access to the right resources for the right reasons

D. All users can reset their own passwords without restrictions

*An identity management system is designed to manage user identities and their access to resources securely and efficiently. The primary goal of such a system is to ensure that the right individuals receive access to the right resources based on their roles, responsibilities, and needs. This involves verifying user identities, assigning appropriate access rights, and monitoring usage to prevent unauthorized access. In this context, the correct answer emphasizes ensuring access is appropriately allocated, which reflects the foundational principle of identity management—granting permission based on established policies and justifications. This not only enhances security by limiting access to sensitive information and systems but also ensures compliance with regulations and organizational standards. The other choices do not accurately describe the purpose of an identity management system. They either imply unrestricted access or lack the necessary checks and balances to maintain security and governance over user privileges.*

SAMPLE

## 7. Which is a benefit of using account lockout policies?

A. It allows users to reset passwords easily

B. It prevents repeated login attempts from attackers

C. It provides immediate access to all users

D. It reduces the number of accounts

*Implementing account lockout policies is critically important in user account management as it serves a primary security function: preventing repeated login attempts from attackers. When an account lockout policy is in place, it temporarily disables a user's account after a certain number of failed login attempts within a designated timeframe. This mechanism is aimed at thwarting brute-force attacks, where an attacker systematically tries different password combinations to gain unauthorized access to an account. By locking the account after a few failed attempts, the system not only increases security but also acts as a deterrent for potential intruders, effectively making it more difficult for them to succeed in their attempts to breach accounts. In contrast, other options don't align with the core purpose of account lockout policies. For instance, allowing users to reset passwords easily is more related to user convenience rather than security; immediate access for all users does not support safety measures; and simply reducing the number of accounts does not pertain to the functioning of account lockout policies. Hence, the key benefit is indeed the prevention of repeated login attempts from attackers, reinforcing the stability and security of the user accounts in the system.*

## 8. How does a user account differ from a group account?

A. A user account is for individuals, while a group account manages multiple users

B. A user account is temporary, while a group account is permanent

C. A user account can have unlimited permissions; a group account cannot

D. A user account is managed by IT, while a group account is user-driven

*A user account is specifically designed to represent an individual user within a system, enabling that person to access and utilize resources based on their assigned permissions. This account usually contains unique credentials and specific settings that apply to the individual. On the other hand, a group account is utilized to manage a collection of user accounts as a single entity. This allows for more efficient administration since permissions and settings can be applied to all members of the group simultaneously, streamlining the process of granting or restricting access to resources based on the group's needs rather than handling each user's account individually. The distinction in purpose between individual user accounts and group accounts is essential for effective user account management. This setup facilitates better organization, especially in larger environments where managing individual permissions for numerous users would be unwieldy.*

SAMPLE

## 9. In Linux, which file contains user account information?

A. /etc/usermap

B. /etc/userinfo

C. /etc/passwd

D. /etc/accounts

*The file that contains user account information in Linux is /etc/passwd. This file is essential for the system as it holds basic details about each user account on the machine. Specifically, it includes the username, user ID (UID), group ID (GID), user information such as the full name, home directory, and the shell associated with the user. The structure of the /etc/passwd file allows for easy retrieval of user information, enabling various system functions related to user authentication and access control. Each line in the file corresponds to a single user account and follows a specific format, which the operating system and applications can interpret. The other choices do not serve this purpose. /etc/usermap, /etc/userinfo, and /etc/accounts are not standard files in Linux systems; they do not traditionally hold user account data as /etc/passwd does. Knowing the significance and role of /etc/passwd is crucial for understanding user account management within a Linux environment.*

## 10. What aspect of password management does a password manager improve?

A. It makes passwords easier to guess

B. It allows sharing passwords between multiple users

C. It promotes strong and unique passwords for different accounts

D. It encourages the use of simple passwords

*A password manager significantly enhances password management by promoting strong and unique passwords for different accounts. This tool generates complex passwords that are difficult to guess, helping users to avoid the pitfalls of reusing the same password across multiple sites. Since many users struggle to remember numerous complex passwords, a password manager securely stores them and automatically fills them in when needed, reducing the likelihood of using weaker, simpler passwords. The overarching benefit is an increased level of security for user accounts, as unique passwords diminish the risk of a potential breach affecting multiple accounts.*

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://useracctmgmt25b.examzify.com

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

SAMPLE