# CYBERARK PRIVILEGED ACCESS SECURITY (PAS) ADMINISTRATION PRACTICE TEST (SAMPLE)

## STUDY GUIDE

## SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

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

https://cyberarkpasadmin.examzify.com

# Table of Contents

# 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

1. **Which of the following steps is NOT part of establishing a session with SSH keys?**

   A. Client and server exchange public keys

   B. The server verifies the client with a password

   C. Both systems agree on a symmetric session key

   D. All further communication is encrypted with the symmetric session key

2. **Which statement is true about the access requirements of Site Support Teams?**

   A. They can access servers without any restrictions

   B. They have unrestricted access during all times

   C. They require management approval to access any server

   D. Access is granted based solely on seniority

3. **What does PSMP stand for in the context of CyberArk?**

   A. Privileged Security Management Proxy

   B. Privileged Security Monitoring Platform

   C. PSM SSH Proxy

   D. Protected Security Management Proxy

4. **What happens to the logs generated in the PSMP flow after the session is recorded?**

   A. Sent to the user's email

   B. Stored in the local drive

   C. Forwarded to SIEM/Syslog

   D. Deleted after review

5. **Master Policy Rules aim primarily to ensure what in the CyberArk Privileged Access Security framework?**

   A. Efficiency in user access

   B. Strict security controls for privileged accounts

   C. Better user management

   D. Increased system awareness

**6. What type of integration does the VaultInternal safe primarily handle?**

A. User authentication

B. LDAP integration

C. Web service connections

D. Data encryption standards

**7. Which setting would restrict a user's access only to the first group they belong to?**

A. Object Level Control

B. Cumulative Privilege

C. DenyOverrides Cumulative Privilege

D. FirstApplicable

**8. What type of definitions does the PVWATaskDefinitions safe contain?**

A. User settings

B. Configurations for system tasks

C. Definitions for reports

D. Encrypted password data

**9. What are the three core functions of PSM?**

A. Authenticate, Authorize, Monitor

B. Isolate, Control, Monitor

C. Manage, Secure, Comply

D. Connect, Control, Isolate

**10. Who defines Vault Authorizations in CyberArk?**

A. System Administrators

B. Only the CyberArk support team

C. Defined via the PrivateArk client

D. Automatically assigned by the system

# Answers

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

# Explanations

## 1. Which of the following steps is NOT part of establishing a session with SSH keys?

A. Client and server exchange public keys

B. The server verifies the client with a password

C. Both systems agree on a symmetric session key

D. All further communication is encrypted with the symmetric session key

*The step involving the server verifying the client with a password is not part of establishing a session with SSH keys. When using SSH keys, the authentication process relies on the cryptographic key pair, where the client possesses a private key and the server holds the corresponding public key. This method allows for secure authentication without the need for password verification, thus streamlining the connection process. In sessions that utilize SSH keys, the client first generates a key pair and shares the public key with the server. When the client attempts to connect, the server uses this public key to confirm the client's identity by checking if it possesses the corresponding private key. This authentication does not require a password, making the process more efficient and secure. The subsequent steps include the exchange of public keys, the agreement on a symmetric session key, and encrypting all further communication with that session key, thereby maintaining confidentiality and integrity throughout the session. These established practices highlight the preference for key-based authentication in SSH setups over traditional password authentication, which can be more vulnerable to attacks.*

## 2. Which statement is true about the access requirements of Site Support Teams?

A. They can access servers without any restrictions

B. They have unrestricted access during all times

C. They require management approval to access any server

D. Access is granted based solely on seniority

*The access requirement indicating that management approval is necessary for Site Support Teams to access any server emphasizes the importance of maintaining security and control over privileged access. This approach reinforces accountability and ensures that access to sensitive systems and data is effectively managed. By requiring management approval, organizations can implement a formal approval process that helps mitigate risks associated with unauthorized access. This requirement is particularly vital in environments where security is paramount, as it ensures that only authorized personnel can access critical resources. It also encourages a culture of oversight, where access is granted based on necessity rather than simply by rank or position. Thus, management can make informed decisions about who should have access, thereby reducing the potential for misuse or errors that could arise from unrestricted access. In contrast, unrestricted access or access based solely on seniority can lead to vulnerabilities, whereas requiring management approval adds a protective layer against unauthorized actions and ensures that access aligns with business needs and security policies.*

## 3. What does PSMP stand for in the context of CyberArk?

A. Privileged Security Management Proxy

B. Privileged Security Monitoring Platform

C. PSM SSH Proxy

D. Protected Security Management Proxy

*In the context of CyberArk, PSMP stands for "Privileged Session Management Proxy." This feature plays a crucial role in managing and securing privileged sessions within the CyberArk privileged access security framework. The PSMP acts as an intermediary between clients and various target systems, ensuring that all privileged sessions are monitored, recorded, and controlled effectively. This enables organizations to enforce security policies, audit access, and maintain compliance in their management of sensitive credentials. By leveraging PSMP, users can connect to servers, applications, and other critical infrastructure in a secure manner while maintaining oversight of these interactions. This helps in reducing risks associated with unauthorized access and ensures that all privileged session activities are logged for auditing purposes. Understanding the functionality provided by PSMP is essential for administrators in implementing robust security measures and managing privileged access effectively within their organizations.*

## 4. What happens to the logs generated in the PSMP flow after the session is recorded?

A. Sent to the user's email

B. Stored in the local drive

C. Forwarded to SIEM/Syslog

D. Deleted after review

*The logs generated in the Privileged Session Manager Proxy (PSMP) flow are essential for security auditing and compliance purposes. After a session is recorded, these logs are typically forwarded to a Security Information and Event Management (SIEM) system or a Syslog server. This process allows for centralized log management, enabling security teams to analyze and monitor privileged access activities effectively. By integrating with SIEM solutions, organizations can correlate the session logs with other security events, enhancing their ability to detect anomalies or potential security breaches. This practice aligns with best practices in cybersecurity, ensuring that critical session data is retained and accessible for future audits and investigations. Other methods of handling logs, such as deleting them after review or storing them on local drives, may compromise security or compliance requirements. Sending logs to a user's email does not provide the necessary oversight or centralized control that SIEM systems offer. Therefore, forwarding logs to SIEM/Syslog is the most effective and secure method of handling session records generated during the PSMP flow.*

## 5. Master Policy Rules aim primarily to ensure what in the CyberArk Privileged Access Security framework?

A. Efficiency in user access

B. Strict security controls for privileged accounts

C. Better user management

D. Increased system awareness

*Master Policy Rules are a fundamental component of the CyberArk Privileged Access Security framework, primarily focused on establishing strict security controls for privileged accounts. These rules are designed to enforce various security protocols, ensuring that access to privileged accounts is managed effectively and that sensitive information is protected against unauthorized access. The emphasis on strict security controls is vital for safeguarding an organization's critical assets. By defining clear policies around password complexity, access durations, and session management, Master Policy Rules help mitigate the risks associated with privileged accounts, which are often primary targets for attackers. This increases the overall security posture of the organization, as it minimizes the potential for insider threats or external breaches through compromised credentials. While factors like efficiency in user access, better user management, and increased system awareness are important for a holistic security strategy, they are typically secondary to the core objective of maintaining stringent security over privileged accounts, which is ultimately prioritized in the framework.*

## 6. What type of integration does the VaultInternal safe primarily handle?

A. User authentication

B. LDAP integration

C. Web service connections

D. Data encryption standards

*The VaultInternal safe is essential for managing and storing sensitive data related to user authentication within the CyberArk system. It primarily handles LDAP (Lightweight Directory Access Protocol) integration, which is crucial for enabling secure access and management of user identities in a centralized directory. This integration is fundamental in ensuring that the users requesting access to privileged accounts are authenticated against an established directory service, facilitating effective identity management and access control across the organization's infrastructure. By storing LDAP connection details and related configurations within the VaultInternal safe, CyberArk enhances security and ensures that the integration remains robust. This implementation allows for seamless communication between CyberArk and the directory services, streamlining user authentication processes, including the verification of user credentials and permissions. This makes the VaultInternal safe an indispensable component in the overall architecture of CyberArk's Privileged Access Security, emphasizing its role in managing user authentication effectively.*

## 7. Which setting would restrict a user's access only to the first group they belong to?

A. Object Level Control

B. Cumulative Privilege

C. DenyOverrides Cumulative Privilege

D. FirstApplicable

*The setting that restricts a user's access only to the first group they belong to is known as "FirstApplicable." This mechanism operates under the principle that when evaluating permissions, CyberArk checks for the access rights assigned to a user based on their memberships in various groups. The access rights assigned to the first applicable group encountered during this evaluation process will take precedence, effectively limiting the user's overall permissions to what is defined in that first group. In practical terms, if a user belongs to multiple groups but is configured with the "FirstApplicable" setting, they will only be granted the rights and privileges defined for their first group, ignoring any additional permissions that may be inherited from subsequent groups. This helps in simplifying access control by ensuring that permissions are not accumulated from multiple sources, thereby promoting a clean and restrictively controlled access environment. This approach contrasts with other settings like cumulative privilege, which would allow a user to accumulate permissions from all groups they belong to, potentially leading to broader access than desired. DenyOverrides cumulative privilege indicates that, while cumulative privilege could apply, any deny rule from a higher priority will override it. Object level control allows for granular permission settings but does not restrict based on group order as "FirstApplicable" specifically does. Thus, "FirstApplicable*

## 8. What type of definitions does the PVWATaskDefinitions safe contain?

A. User settings

B. Configurations for system tasks

C. Definitions for reports

D. Encrypted password data

*The PVWATaskDefinitions safe contains configurations for system tasks. This safe is primarily focused on storing and managing the definitions required for various automated tasks that the CyberArk Vault can perform. These task definitions include parameters and specifications necessary for the execution of tasks essential to the governance and management of privileged accounts. In CyberArk, proper task definitions are crucial for ensuring that automated workflows operate smoothly, securely, and effectively. This includes scheduling tasks such as password rotations, automatic updates, or compliance-related activities. Understanding the role of the PVWATaskDefinitions safe is important for administrators as it allows them to manage and customize the execution of system-level tasks that further enhance security and operational efficiency within the organization. The other options describe different functionalities that are not associated with the PVWATaskDefinitions safe and do not reflect its purpose in the context of CyberArk's architecture. User settings pertain to individual preferences rather than system task configurations, report definitions are more about data extraction and presentation, and encrypted password data is specifically handled in other areas of the CyberArk Vault system.*

## 9. What are the three core functions of PSM?

A. Authenticate, Authorize, Monitor

B. Isolate, Control, Monitor

C. Manage, Secure, Comply

D. Connect, Control, Isolate

*The correct answer emphasizes the core functions of Privileged Session Manager (PSM) within CyberArk's Privileged Access Security framework. PSM plays a critical role in managing privileged sessions by ensuring security and compliance are maintained during remote access. The function "Isolate" pertains to the ability of PSM to create a secure environment for privileged access, effectively separating the session from the user's local environment and protecting systems from potential threats associated with remote sessions. "Control" refers to the regulation and management of user access and actions during a privileged session. It ensures that only authorized personnel can access sensitive systems and that all actions taken can be monitored and audited for compliance. "Monitor" is about the real-time tracking of privileged sessions, allowing administrators to observe activities during access and ensure that no unusual or unauthorized actions are carried out. This function is critical for compliance and for detecting any suspicious behavior that could lead to a security breach. Each of these functions works together to bolster security, control access, and ensure that the organization meets necessary compliance standards while managing privileged credentials effectively.*

## 10. Who defines Vault Authorizations in CyberArk?

A. System Administrators

B. Only the CyberArk support team

C. Defined via the PrivateArk client

D. Automatically assigned by the system

*The correct answer is that vault authorizations are defined via the PrivateArk client. In CyberArk, the PrivateArk client is a tool used by administrators to manage and configure various aspects of the vault, including authorizations. This means that system administrators can use the graphical interface of the PrivateArk client to specify which users or user groups have access to different resources within the vault, enabling them to control permissions and ensure security compliance. Using the PrivateArk client provides a level of customization and flexibility that allows administrators to align vault access with the organization's security policies and operational needs. This process is crucial for safeguarding sensitive information and managing privileged access effectively. Other choices, such as only the CyberArk support team being responsible for defining vault authorizations, do not reflect the role of a system administrator who actively manages access controls. The option stating that authorizations are automatically assigned by the system also misrepresents the nature of vault authorization management, as it requires deliberate configuration rather than an automatic process.*

# 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://cyberarkpasadmin.examzify.com

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