

WORKDAY SECURITY PRACTICE TEST (SAMPLE)

STUDY GUIDE



Prepare with structure. Pass with confidence



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.

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 Workday component allows for the view of user access permissions?**
 - A. The Security Console
 - B. The User Admin Dashboard
 - C. The Compliance Monitor
 - D. The Access Control Panel

- 2. True or False: You can create security rules based on any report field in Workday.**
 - A. True
 - B. False
 - C. Only for custom fields
 - D. Only if you have full access rights

- 3. What action ensures that a user sees only specific Ledger Account values when running the Trial Balance report?**
 - A. Set up ledger account security segments
 - B. Use global security settings
 - C. Enable system-wide access controls
 - D. Assign full ledger access

- 4. What does the term 'Separation of Duties' refer to in Workday Security?**
 - A. A measure to combine all tasks under one user
 - B. A strategy to minimize risk by dividing tasks among users
 - C. A protocol that allows one user to approve all transactions
 - D. An approach to reduce user accountability

- 5. True or False: Security permissions in Workday can only be modified by administrators.**
 - A. True
 - B. False
 - C. Only by selected users
 - D. None of the above

- 6. What role does the report owner play in relation to the visibility of custom reports?**
- A. They determine the report content
 - B. They define data sources
 - C. They control who can view the report
 - D. They manage report scheduling
- 7. For whom is the constrained proxy feature specifically beneficial?**
- A. Administrators who need help
 - B. Any user needing temporary assignments
 - C. All employees
 - D. Report builders only
- 8. What is the process for revoking user access in Workday?**
- A. By removing the user from the organization completely.
 - B. Through user security group removal or role reassignment.
 - C. By notifying the user directly of the revocation.
 - D. By creating a log of all access attempts.
- 9. What determines which target data a security group member sees when accessing a secured item?**
- A. The security policy restrictions
 - B. The secured item permission required
 - C. The security group context type
 - D. The functional area
- 10. What is the function of the Session Timeout property in Workday?**
- A. To enhance internet speed for users
 - B. To automatically log users out after inactivity
 - C. To allow multiple users to access accounts simultaneously
 - D. To remind users of pending tasks

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which Workday component allows for the view of user access permissions?

- A. The Security Console**
- B. The User Admin Dashboard
- C. The Compliance Monitor
- D. The Access Control Panel

The Security Console is the correct choice because it is specifically designed to manage and view user security settings, including access permissions within Workday. This component provides administrators with a comprehensive view of user roles and the permissions assigned to each role, allowing for effective oversight and management of security within the system. In the Security Console, administrators can also define and adjust user access to various Workday functionalities and data, ensuring that users have appropriate permissions based on their job responsibilities. This centralized control is crucial for maintaining data security and regulatory compliance, as it helps ensure that sensitive information is only accessible to those who need it. Other components such as the User Admin Dashboard, Compliance Monitor, and Access Control Panel serve different functions related to user management or compliance monitoring but do not primarily focus on providing a detailed view of user access permissions in the way that the Security Console does.

2. True or False: You can create security rules based on any report field in Workday.

- A. True
- B. False**
- C. Only for custom fields
- D. Only if you have full access rights

In Workday, the ability to create security rules is limited to specific fields that are part of the system's data model. This means you cannot create security rules based on just any report field. Instead, security rules are typically restricted to predefined fields that the system recognizes for security purposes. This limitation ensures that sensitive data is adequately protected and that security configurations do not become overly complex or unmanageable. Creating security rules allows organizations to control access to data based on business needs, ensuring users only see information relevant to their roles. However, since not every report field in Workday is configured for security rules, it is inaccurate to claim that any report field can be utilized for this purpose. The focus on specific fields helps streamline security management and maintain the integrity of sensitive data within the platform.

3. What action ensures that a user sees only specific Ledger Account values when running the Trial Balance report?

- A. Set up ledger account security segments**
- B. Use global security settings
- C. Enable system-wide access controls
- D. Assign full ledger access

Setting up ledger account security segments is the correct action to ensure that a user sees only specific Ledger Account values when running the Trial Balance report. By implementing these security segments, you can define which ledger accounts are visible to different users or user groups based on their role or data access needs. This targeted approach allows organizations to maintain control over financial data, ensuring users can only view information that is relevant to their specific job functions or requirements. This method supports compliance and minimizes the risk of unauthorized access to sensitive financial information. It also simplifies the user experience by filtering out irrelevant data, enabling users to focus on the accounts pertinent to their responsibilities. Other options such as global security settings and system-wide access controls are broader approaches that impact multiple areas of security and may not provide the granularity needed for ledger account visibility. Similarly, assigning full ledger access would grant users access to all ledger accounts, which contradicts the intention of displaying only specific values.

4. What does the term 'Separation of Duties' refer to in Workday Security?

- A. A measure to combine all tasks under one user
- B. A strategy to minimize risk by dividing tasks among users**
- C. A protocol that allows one user to approve all transactions
- D. An approach to reduce user accountability

The term 'Separation of Duties' in Workday Security refers to a strategy aimed at minimizing risk by dividing tasks among multiple users. This principle is fundamental to organizational security because it helps prevent fraud and errors. By ensuring that no single user has control over all aspects of any critical business process, organizations can create a system of checks and balances. This approach can help mitigate the risk of intentional misconduct or accidental mistakes since different individuals are involved in the various stages of a transaction or task. When tasks are distributed among various users, it not only enhances security but also promotes accountability within the organization. Each user is responsible for their specific tasks, which helps track activity more effectively and allows for a more thorough audit trail. In contrast, the other options present practices that do not align with security best practices. Combining all tasks under one user or allowing one user to approve all transactions can create significant vulnerabilities, as these scenarios concentrate too much power and responsibility in the hands of a single individual. Similarly, an approach that reduces user accountability undermines the fundamental goals of effective governance and security, making it easier for issues to arise without clear ownership or oversight.

5. True or False: Security permissions in Workday can only be modified by administrators.

- A. True**
- B. False
- C. Only by selected users
- D. None of the above

The statement that security permissions in Workday can only be modified by administrators is indeed true. In Workday, security is a critical aspect of application management, and to maintain the integrity and safety of sensitive information, only authorized individuals, typically administrators, have the necessary permissions to make changes to security settings. Administrators have the responsibility to ensure that data is accessed in compliance with organizational policies and security protocols. This includes granting or restricting access based on roles and responsibilities within the organization. By limiting the modification of security permissions to administrators, Workday helps prevent unauthorized access and potential data breaches, ensuring that sensitive information remains secure. In Workday, while there may be roles within the platform that can perform certain actions related to security, none of those roles would possess the same level of access and permission management as an administrator. Therefore, the control over security permissions is intentionally designated to admins to uphold best practices in data security.

6. What role does the report owner play in relation to the visibility of custom reports?

- A. They determine the report content
- B. They define data sources
- C. They control who can view the report**
- D. They manage report scheduling

The report owner has a crucial responsibility when it comes to the visibility of custom reports. Specifically, they control who can view the report by setting appropriate security controls and sharing settings within Workday. This means that the report owner can restrict access to specific user roles, groups, or individuals based on business needs or data sensitivity. By managing these permissions, the report owner ensures that only authorized personnel have access to the report's data, safeguarding confidential information and maintaining proper data governance. While other roles may involve determining report content, defining data sources, or managing report scheduling, these responsibilities do not pertain to the visibility aspect directly. Therefore, the powerful role of the report owner primarily revolves around controlling access, making it a key element in the overall security and utility of the reporting function within Workday.

7. For whom is the constrained proxy feature specifically beneficial?

- A. Administrators who need help**
- B. Any user needing temporary assignments
- C. All employees
- D. Report builders only

The constrained proxy feature primarily benefits administrators who need assistance in managing tasks within Workday. This feature allows designated users to act on behalf of another user while limiting the scope of actions they can perform. For administrators, this is particularly valuable because it enables them to delegate specific responsibilities and tasks to other individuals without compromising the entirety of an administrator's permissions. The constrained proxy ensures that administrative functions can be carried out efficiently, with control over which actions the proxy can execute, reducing the risk of errors or unauthorized activities. This targeted delegation is crucial in maintaining security and compliance within the organization's data management framework. While temporary assignments and collaborations may be helpful to any user or specific roles like report builders, the unique constraints placed on the proxy feature are designed with administrators' need for focused assistance in mind, making their workflows smoother while still safeguarding sensitive information.

8. What is the process for revoking user access in Workday?

- A. By removing the user from the organization completely.
- B. Through user security group removal or role reassignment.**
- C. By notifying the user directly of the revocation.
- D. By creating a log of all access attempts.

The process for revoking user access in Workday primarily involves user security group removal or role reassignment. This approach is effective because Workday utilizes security groups and roles to manage permissions and access within the system. When a user is removed from a specific security group, they lose the associated access rights that group confers. Reassigning roles can also modify or eliminate the permissions a user has, ensuring that only authorized users retain access to certain data or functions. This method aligns with best practices in security management where access is tightly controlled and adjusted based on user roles and group memberships rather than resorting to more drastic measures, such as completely removing the user from the organization or directly notifying them of access changes. Additionally, logging access attempts is useful for compliance and monitoring but does not constitute a method for immediate revocation of user access.

9. What determines which target data a security group member sees when accessing a secured item?

- A. The security policy restrictions
- B. The secured item permission required
- C. The security group context type**
- D. The functional area

The correct answer focuses on the significance of the security group context type in determining what target data a member of a security group can access. Security group context type refers to the specific context within which a security group operates, and it plays a critical role in defining the visibility of data related to secured items. When a member accesses secured items, the context type outlines what data within that item is visible to them based on their group affiliations. This means that the configuration of a security group's context dictates the data permissions assigned, resulting in a tailored experience for different users depending on their roles, responsibilities, and group memberships. In contrast, while security policy restrictions and secured item permissions influence access rights by defining the bounds of what the security group can access, these aspects do not specifically dictate the actual target data seen by members. The functional area may pertain to the operational domain but does not have a direct relationship with the visibility of individual data items, which is fundamentally linked to the context type of the security group.

10. What is the function of the Session Timeout property in Workday?

- A. To enhance internet speed for users
- B. To automatically log users out after inactivity**
- C. To allow multiple users to access accounts simultaneously
- D. To remind users of pending tasks

The Session Timeout property in Workday is designed to automatically log users out of the system after a period of inactivity. This function is crucial for maintaining the security of sensitive information and ensuring that unauthorized individuals cannot access an active session if the user becomes inactive or leaves their workstation unattended. By implementing a timeout period, Workday mitigates the risk of data breaches due to forgotten logouts, promoting a safer environment for managing and accessing personal and organizational data. The focus on security through session management is particularly important in modern applications where data protection is a priority. The feature reinforces best practices in user session handling, aligning with compliance standards and organizational policies aimed at safeguarding information.

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://workdaysecurity.examzify.com>

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

SAMPLE