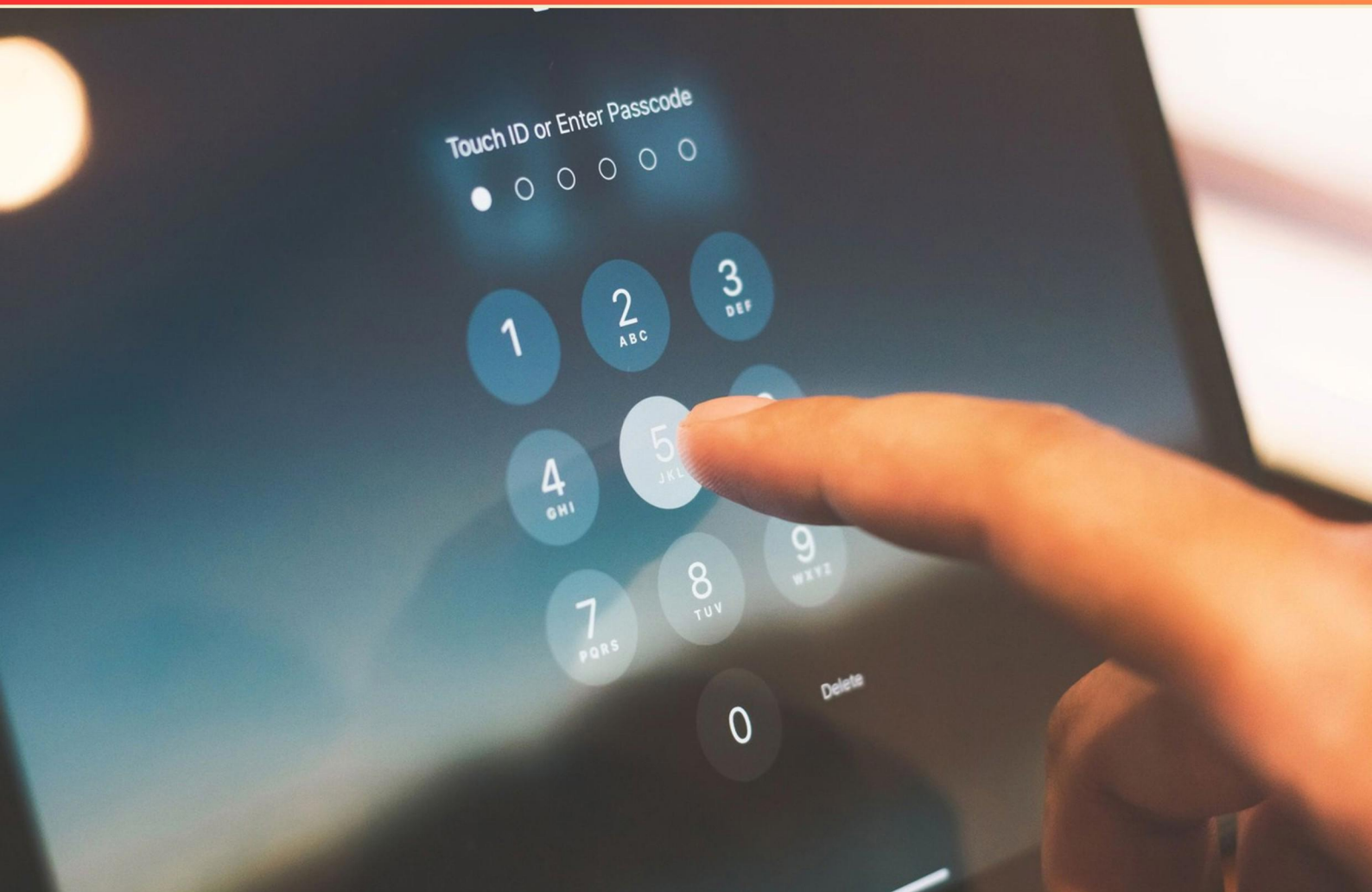


SAILPOINT IDENTITY NOW (IDN) PROFESSIONAL PRACTICE EXAM (SAMPLE) STUDY GUIDE



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	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 distinguishes Authoritative Sources in IdentityNow?**
 - A. They are solely for financial data
 - B. They are the systems of record for user information
 - C. They are used only for troubleshooting
 - D. They are temporary data storage systems
- 2. What occurs if a source fails during the Password Synchronisation process?**
 - A. All changes are rolled back to the previous password
 - B. A failure notification is sent, but successful changes remain
 - C. The user is prompted to retry the password change
 - D. All processes are halted until the error is fixed
- 3. In the context of IdentityNow, who is defined as an identity?**
 - A. A role within the organization
 - B. A user in IdentityNow
 - C. A system for data storage
 - D. An external stakeholder
- 4. What is crucial for the successful operation of password sync groups?**
 - A. Each source must share a common user interface
 - B. Each source must have the same password policy
 - C. Users must change passwords at the same time
 - D. All sources must support multi-factor authentication
- 5. How often are reminder notifications sent until a campaign ends?**
 - A. Every day
 - B. Every week
 - C. Every month
 - D. Only at the beginning of the campaign

- 6. Where should you look to find a record of all provisioning actions sent to the Directory in the last seven days?**
- A. Provisioning summary report
 - B. Account Activity search
 - C. Application audit log
 - D. User activity dashboard
- 7. What is a primary benefit of AI services in identity management?**
- A. Enables automatic password generation
 - B. Improves decision-making for access requests
 - C. Eliminates the need for user passwords
 - D. Replaces manual authentication processes
- 8. What are the four primary processes of IdentityNow?**
- A. Approval, Provisioning, Data Reading, Governance
 - B. Reading Data, Business Modelling, Provisioning, Governance
 - C. Access Control, Data Reading, User Management, Reporting
 - D. Data Importing, User Approval, System Integration, Governance
- 9. Which of the following components cannot utilize transforms?**
- A. API integrations
 - B. Identity management features
 - C. Connectors
 - D. Reporting functionalities
- 10. In IdentityNow, who is responsible for reviewing requests in a Governance Group?**
- A. Only the manager of the requestor
 - B. Only the system administrator
 - C. Any member assigned to the Governance Group
 - D. No one; requests are auto-approved

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What distinguishes Authoritative Sources in IdentityNow?

- A. They are solely for financial data
- B. They are the systems of record for user information**
- C. They are used only for troubleshooting
- D. They are temporary data storage systems

Authoritative Sources in IdentityNow are critical because they serve as the primary systems of record for user information. This means they contain the most accurate and up-to-date data regarding users' identities, roles, access rights, and other relevant attributes. The integrity and reliability of the information in these sources are essential for effective identity management. In an identity governance context, having a definitive source of truth is crucial for ensuring that identity data is consistent and trustworthy across the organization's various applications and systems. Authoritative Sources often include HR systems, directory services, and other key databases that manage user identities. In contrast, the other options do not accurately represent the nature of Authoritative Sources. For example, they are not limited strictly to financial data, so the concept of being tied solely to financial information is incorrect. Authoritative Sources also play a role in ongoing identity operations rather than being used exclusively for troubleshooting. Finally, they are not temporary data storage systems, as their purpose is to maintain persistent and reliable records rather than serving as short-term storage.

2. What occurs if a source fails during the Password Synchronisation process?

- A. All changes are rolled back to the previous password
- B. A failure notification is sent, but successful changes remain**
- C. The user is prompted to retry the password change
- D. All processes are halted until the error is fixed

In the scenario where a source fails during the Password Synchronization process, the system is designed to ensure that successful changes remain intact while providing a notification about the failure. This is crucial for maintaining user experience and system integrity. Implementing a rollback without a prompt to preserve successful changes could lead to unnecessary rejections of valid updates and create frustration for users. The rationale behind this approach emphasizes efficiency; it allows for partial successes to be maintained so that users are not locked out of their accounts or forced to repeat steps unnecessarily. Meanwhile, sending a failure notification alerts administrators or relevant personnel to investigate the issue without disrupting the entire process. This balances functionality and user convenience during synchronization tasks, leading to a more resilient system architecture.

3. In the context of IdentityNow, who is defined as an identity?

- A. A role within the organization
- B. A user in IdentityNow**
- C. A system for data storage
- D. An external stakeholder

In IdentityNow, an identity is defined as a user within the platform. This reflects the core function of IdentityNow, which is centered around managing user identities and access rights across various systems and applications. Each identity represents a unique user, including their associated data, credentials, roles, and entitlements. When considering the other options, while roles within the organization play a significant part in managing permissions and access (they define what a user can do), they do not represent an identity in the IdentityNow context. Similarly, a system for data storage is a component that IdentityNow uses to hold identity data but does not make up an identity itself. Lastly, external stakeholders may interact with organizational systems, but they are not considered identities unless they are defined as users in the identity management framework. Hence, the most accurate definition of an identity in this context is indeed a user in IdentityNow.

4. What is crucial for the successful operation of password sync groups?

- A. Each source must share a common user interface
- B. Each source must have the same password policy**
- C. Users must change passwords at the same time
- D. All sources must support multi-factor authentication

The successful operation of password sync groups significantly relies on the requirement that each source must have the same password policy. This consistency is vital because it ensures that passwords comply with the same complexity, length, and expiration requirements across all systems involved. If each source has differing password policies, it would be challenging to synchronize passwords seamlessly; users might encounter issues when attempting to log in or may face situations where passwords are not updated correctly across the systems. This uniformity across password policies allows for a smoother experience for users who might be managing multiple accounts, as they will only need to follow one set of rules when creating or updating passwords, thereby reducing confusion and potential errors. In environments where password sync is implemented, ensuring this commonality enables reliable and secure synchronization, fostering a more cohesive identity management strategy.

5. How often are reminder notifications sent until a campaign ends?

- A. Every day
- B. Every week**
- C. Every month
- D. Only at the beginning of the campaign

Reminder notifications are typically sent every week until a campaign ends. This frequency allows participants ample time to respond or complete necessary actions without overwhelming them with daily reminders. Weekly reminders strike a balance between keeping the campaign's goals at the forefront of participants' minds and giving them enough time to address the tasks at hand. This approach also aligns with best practices in campaign management, ensuring sustained engagement without being intrusive. By using weekly reminders, the campaign can maintain momentum and encourage participation throughout its duration.

6. Where should you look to find a record of all provisioning actions sent to the Directory in the last seven days?

- A. Provisioning summary report
- B. Account Activity search**
- C. Application audit log
- D. User activity dashboard

The best source for finding a record of all provisioning actions sent to the Directory in the last seven days is the Account Activity search. This feature is specifically designed to track and report on the provisioning actions associated with user accounts. Through this search function, you can narrow down the timeframe to view actions taken in the last seven days, providing a clear and detailed history of the account activity relevant to provisioning. The Account Activity search is tailored for this purpose, allowing users to access logs regarding the creation, modification, and deletion of accounts within the Identity Now environment. This makes it the most suitable choice for examining recent provisioning actions. Other options, while potentially useful for different aspects of identity management and auditing, do not focus specifically on the recent provisioning actions. For instance, the Provisioning summary report can provide overall statistics on provisioning actions but may not offer the granular detail for the last seven days that the Account Activity search does. The Application audit log typically records broader system-level events rather than specific account provisioning actions. The User activity dashboard may present an overview of user-related actions but is not specifically aimed at auditing provisioning history.

7. What is a primary benefit of AI services in identity management?

- A. Enables automatic password generation
- B. Improves decision-making for access requests**
- C. Eliminates the need for user passwords
- D. Replaces manual authentication processes

The primary benefit of AI services in identity management lies in their ability to enhance decision-making for access requests. AI can analyze vast amounts of data to recognize patterns and determine risk levels associated with user behavior and access requests. By leveraging machine learning algorithms, AI can provide insights that help administrators quickly assess and manage user privileges, ensuring that access is granted only when appropriate and based on context, such as user roles, behavioral anomalies, and historical access patterns. This capability is particularly valuable in today's complex environments where threats can emerge from various angles, and the stakes of access management are higher than ever. The AI's ability to process data in real-time allows organizations to respond faster to potential security incidents and maintain compliance with various regulations by ensuring that users have the appropriate access levels. While options like automatic password generation or the elimination of user passwords might sound beneficial, they do not encapsulate the comprehensive decision-making advantages that AI brings to identity management processes. Similarly, although replacing manual authentication processes is a goal for many organizations, it is not the primary benefit of implementing AI services; instead, it focuses primarily on efficiency rather than intelligence in decision-making.

8. What are the four primary processes of IdentityNow?

- A. Approval, Provisioning, Data Reading, Governance
- B. Reading Data, Business Modelling, Provisioning, Governance**
- C. Access Control, Data Reading, User Management, Reporting
- D. Data Importing, User Approval, System Integration, Governance

The identification of the four primary processes of IdentityNow highlights core functionalities essential for effective identity governance and administration. The correct choice emphasizes the processes of Reading Data, Business Modelling, Provisioning, and Governance. Reading Data refers to the capability of the system to gather and manage identity data from various sources. This foundational step is crucial for understanding who has access to what resources and for ensuring that the identity information is accurate and up-to-date. Business Modelling allows organizations to define how roles and entitlements are structured, which informs how users will be granted access to applications and resources based on their job functions. This process is vital for aligning access rights with business requirements. Provisioning is the process of creating, modifying, and removing user access to resources based on policy decisions and ongoing changes in roles or employment status. This ensures that users have the access they need while also maintaining security by preventing unauthorized access. Governance involves overseeing and ensuring compliance with access controls, policies, and regulations within the organization. It helps maintain accountability and security by monitoring user access and conducting regular audits. These processes collectively support a comprehensive identity management strategy, allowing organizations to effectively manage user identities and their corresponding access in a secure and compliant manner.

9. Which of the following components cannot utilize transforms?

- A. API integrations
- B. Identity management features
- C. Connectors**
- D. Reporting functionalities

The ability to utilize transforms is integral to certain components of SailPoint Identity Now, particularly for those that involve data manipulation or data flows. Connectors serve as bridges between Identity Now and various endpoints, and they primarily function to facilitate data synchronization rather than transformation. While connectors may extract, load, and sync data, they do not typically involve complex data transformations that would excuse the need to use transforms. On the other hand, API integrations, identity management features, and reporting functionalities benefit from transforms. API integrations can use transforms to modify the data sent or received, enhancing interoperability between systems. Identity management features often rely on transforms to tailor identity data according to specific requirements or business rules, allowing for more granular control over identity lifecycles. Similarly, reporting functionalities use transforms to present data in formats that make it more digestible and useful for analysis. Thus, connectors are the component that cannot utilize transforms, as their primary role is to connect and ensure data flow between systems rather than change the structure or content of the data involved.

10. In IdentityNow, who is responsible for reviewing requests in a Governance Group?

- A. Only the manager of the requestor
- B. Only the system administrator
- C. Any member assigned to the Governance Group**
- D. No one; requests are auto-approved

In IdentityNow, the responsibility for reviewing requests in a Governance Group falls to any member assigned to that group. This approach fosters collaboration and ensures that a diverse pool of perspectives is considered when evaluating access requests. By allowing any member of the Governance Group to participate in the review process, the system enhances the overall governance and compliance posture by leveraging the expertise and knowledge of multiple individuals. The Governance Group is designed to include representatives who understand the requirements and risks associated with granting access to systems and data. This inclusive model helps mitigate risks associated with potential conflicts of interest, as multiple views and checks are in place before approval is granted. It empowers team members to share their insights and ensure that access is appropriate based on organizational policies and security protocols. In contrast, limiting reviews to only the manager of the requestor or solely to a system administrator can create bottlenecks or risks due to a lack of comprehensive assessment. Automatic approval of requests would undermine the governance framework, potentially leading to security vulnerabilities and unmonitored access, as no consideration would be given to the implications of granting such access.

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://sailpointidentitynowprofessional-idn.examzify.com>

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

SAMPLE