# Salesforce Sharing and Visibility Certification Practice Exam (Sample)

## Study Guide

BY EXAMZIFY

**Everything you need from our exam experts!**

Sample study guide. For the full version with hundreds of questions, visit:
https://salesforce-sharingandvisibility.examzify.com

**Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.**

# 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. When trying to implement parallel processes within Salesforce, what activity poses minimal risk related to group membership locking?**

**A. Creating a new Role.**

**B. Deleting a Role.**

**C. Editing existing Roles.**

**D. Transforming existing Roles into Territories.**

**2. Which method would allow viewing of encrypted custom field contents in clear text?**

**A. Stack trace viewer in the developer console**

**B. Trigger field update copying encrypted field to unencrypted field**

**C. Debug log output from system.debug(object.encryptedField__c)**

**D. Webservice that returns secret as a string**

**3. Which method can be used to enforce user permissions at the object level?**

**A. Schema.DescribeSObjectResult**

**B. UserInfo.getUserRole**

**C. Schema.getObjectDescribe**

**D. Schema.DescribeAccountResult**

**4. How can record visibility be crucial to user collaboration in Salesforce?**

**A. It limits teamwork by restricting user interactions.**

**B. It permits users to access only their records.**

**C. It allows users to access relevant records, enhancing cooperative work.**

**D. It keeps all records private for data security.**

**5. What type of security vulnerability is indicated by using escape="false" in a Visualforce output?**

**A. SOQL Injection**

**B. Access Control**

**C. Arbitrary Redirects**

**D. Cross-Site Scripting**

**6. How can the Architect ensure that only support representatives can access a private key in a managed package while preventing partners from doing so?**

- **A. Store the value in a text field on a protected custom setting.**
- **B. Store the value in a static variable in a class included in the managed package.**
- **C. Store the value in a text field on a list custom setting.**
- **D. Store the value in an encrypted field on a custom object in the package.**

**7. What type of access does the OWD (Organization-Wide Default) setting define?**

- **A. Global settings for all objects**
- **B. Baseline level of access regardless of user role**
- **C. Temporary access for users during training**
- **D. Individual object settings only for managers**

**8. What approach should a manager at Ursa Major Solar use to validate sharing and visibility changes?**

- **A. Use Administrative and User reports to view the Active Users.**
- **B. Use the Login As feature for a sample user in each role and profile.**
- **C. Use Field Audit Trail to audit the field meta-data and visibility.**
- **D. Use the Sharing button to test Profile and Permission set changes.**

**9. What step should an Architect take to ensure the Director of Support has access to all Reimbursement records?**

- **A. Leave the Reimbursement Object in "Deployed" Status and set the Director of Supports Profile to "View All" in the object permissions**
- **B. Use an Approval Process to change the owner of the Reimbursement record upon submission to the Director of Support**
- **C. Disable Grant Access Using Hierarchies for the Object and create a Sharing Rule to enable sharing to the Director of Support**
- **D. Implement a public group that includes the Director of Support**

**10. How can an architect ensure object-level security is enforced in a Visualforce Application that uses a custom Apex Controller?**

- **A. Utilize the "With Sharing" keyword when defining the Visualforce Page**
- **B. Use the Schema.DescribeSObjectResult isAccessible() method in the Apex Controller**
- **C. Utilize the "Without Sharing" keyword when defining the Apex Controller Class**
- **D. Use the "With Sharing" keyword when defining the Apex Controller Class**

# Answers

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

# Explanations

## 1. When trying to implement parallel processes within Salesforce, what activity poses minimal risk related to group membership locking?

A. Creating a new Role.

B. Deleting a Role.

C. Editing existing Roles.

D. Transforming existing Roles into Territories.

**Creating a new Role poses minimal risk related to group membership locking because it does not affect any existing roles or their associated users. When a new role is added, it simply expands the hierarchical structure without interfering with current relationships or memberships. This action allows for more flexibility in organizing users without risking any interruptions in access or visibility that could occur when modifying or deleting existing roles, which may require re-evaluating group memberships and could result in unexpected outcomes. In contrast, deleting a role or editing existing roles can lead to group membership locks, as these actions directly impact the existing users associated with those roles. Transforming roles into territories could also introduce complexity and risk, as it alters the fundamental structure of how users are grouped and their visibility settings. Thus, creating a new role is a low-risk activity within parallel processes in Salesforce.**

## 2. Which method would allow viewing of encrypted custom field contents in clear text?

A. Stack trace viewer in the developer console

B. Trigger field update copying encrypted field to unencrypted field

C. Debug log output from system.debug(object.encryptedField__c)

D. Webservice that returns secret as a string

**The method that allows viewing of encrypted custom field contents in clear text is through a trigger field update that copies the encrypted field to an unencrypted field. When data is encrypted in Salesforce, it is stored securely to protect sensitive information, but there are situations where you may need to access that data in its original, readable format. By creating a trigger that updates a separate unencrypted field with the value from the encrypted field, you can retrieve and view the sensitive data in clear text when required. This method is effective because it adheres to Salesforce's security model and data protection policies, allowing you to handle sensitive information safely. In contrast, other options have limitations regarding security and visibility. For instance, using a stack trace viewer or debug logs may display a reference or the encrypted value but not the actual clear text. Debug logs and web services that expose sensitive data as a string could lead to potential vulnerabilities or compliance issues, as they do not provide a secure way to display the content of encrypted fields. The trigger method is both compliant and practical for such needs.**

## 3. Which method can be used to enforce user permissions at the object level?

A. Schema.DescribeSObjectResult

B. UserInfo.getUserRole

C. Schema.getObjectDescribe

D. Schema.DescribeAccountResult

**The method that can be used to enforce user permissions at the object level is Schema.DescribeSObjectResult. This method is part of the Schema namespace in Salesforce and allows developers to retrieve metadata about an object, which includes information on field permissions and object permissions for the current user's profile and permission sets. By leveraging this method, developers can check whether a user has permission to access or manipulate records for a specific object, thus enabling fine-grained control over data visibility and user actions based on their assigned permissions. While other methods like UserInfo.getUserRole provide insights into user roles, they do not directly enforce or check object-level permissions. Schema.getObjectDescribe and Schema.DescribeAccountResult offer metadata details but are more specific and do not encompass the comprehensive capabilities required to assess object-level permissions the way DescribeSObjectResult does. Therefore, using Schema.DescribeSObjectResult is the most effective approach for enforcing user permissions at the object level.**

## 4. How can record visibility be crucial to user collaboration in Salesforce?

A. It limits teamwork by restricting user interactions.

B. It permits users to access only their records.

C. It allows users to access relevant records, enhancing cooperative work.

D. It keeps all records private for data security.

**Record visibility plays a vital role in fostering collaboration among users in Salesforce by allowing them to access relevant records that are necessary for their cooperative efforts. When users can see and interact with pertinent information, they are better equipped to work together towards common goals, make informed decisions, and contribute effectively to team projects. This access enables sharing of insights, streamlining communication, and reducing the need for unnecessary approvals or information requests, ultimately promoting a collaborative work environment. In this context, record visibility ensures that team members can easily find and utilize the data they need to perform their tasks, thereby enhancing teamwork and productivity. By making relevant records accessible, Salesforce supports a more integrated approach to collaboration, facilitating shared knowledge and efficient workflows among users.**

## 5. What type of security vulnerability is indicated by using escape="false" in a Visualforce output?

A. SOQL Injection

B. Access Control

C. Arbitrary Redirects

D. Cross-Site Scripting

Using escape="false" in a Visualforce output poses a security vulnerability related to Cross-Site Scripting (XSS). When escape="false" is utilized, it allows dynamic content to be rendered directly into the HTML without escaping potentially harmful scripts. As a result, if an attacker manages to inject malicious JavaScript or HTML code into the output, it could be executed in the context of a user's browser, leading to unauthorized actions or data theft.  Cross-Site Scripting occurs when an application includes untrusted data on a web page without proper validation or escaping, allowing attackers to inject scripts that can manipulate user sessions, redirect users to malicious sites, or perform unauthorized actions on behalf of users. Therefore, it is crucial to use escape="true" (or omit the escape attribute as it defaults to true) for any user-generated or externally sourced content to prevent this vulnerability and protect the integrity and security of the application.

## 6. How can the Architect ensure that only support representatives can access a private key in a managed package while preventing partners from doing so?

A. Store the value in a text field on a protected custom setting.

B. Store the value in a static variable in a class included in the managed package.

C. Store the value in a text field on a list custom setting.

D. Store the value in an encrypted field on a custom object in the package.

The correct choice revolves around utilizing a static variable in a class included in the managed package because it efficiently restricts access to the data while maintaining usability. When the key is stored in a static variable, it is encapsulated within the class, ensuring that it cannot be accessed directly from outside the managed package, such as by partners or other external users. The managed package provides a boundary that contains its components, thereby limiting visibility.  This approach leverages the encapsulation features of Apex, ensuring that only the classes defined within the package can utilize this static key. It allows the support representatives, who have access to the managed package classes, to retrieve the key securely without exposing it to unauthorized users or partners.  Other options, like storing the key in custom settings or objects, don't provide the same level of security. For instance, custom settings can be accessed by users with broader permissions, potentially allowing partners to reach sensitive data if they have appropriate access to the settings. Similarly, while an encrypted field on a custom object can secure data at rest, it may still not provide fine-grained access control, as partners could potentially be granted access to that object depending on the sharing rules in place.  Therefore, utilizing a static variable in a class restricts access to the

## 7. What type of access does the OWD (Organization-Wide Default) setting define?

A. Global settings for all objects

B. Baseline level of access regardless of user role

C. Temporary access for users during training

D. Individual object settings only for managers

The Organization-Wide Default (OWD) setting establishes the baseline level of access that users have to records in Salesforce, regardless of their role or profile. This fundamental access level applies to all records of a given object and serves as the minimum permission that can be configured for a user accessing those records. When OWD is set, it determines whether users can see, edit, or share records that they do not own based on the defined settings—options typically include Private, Public Read Only, or Public Read/Write. This makes it critical for maintaining data security and appropriate sharing practices within an organization, as it sets a foundational framework for how access is governed. Other options do not accurately describe the purpose of OWD. Global settings for all objects suggest a broader, more all-encompassing control mechanism, while temporary training access implies a limited-time adjustment that is outside the scope of OWD. Individual object settings for managers suggest a more specific application rather than the overarching nature of OWD settings, which applies uniformly to all users.

## 8. What approach should a manager at Ursa Major Solar use to validate sharing and visibility changes?

A. Use Administrative and User reports to view the Active Users.

B. Use the Login As feature for a sample user in each role and profile.

C. Use Field Audit Trail to audit the field meta-data and visibility.

D. Use the Sharing button to test Profile and Permission set changes.

The approach of using the Login As feature for a sample user in each role and profile is particularly effective for validating sharing and visibility changes because it allows the manager to directly experience the Salesforce interface from the perspective of different users. By logging in as specific users, the manager can quickly ascertain what data the users can see and access, ensuring that the changes made to roles, profiles, and permissions are functioning as intended. This method provides a real-time and practical way to test the effectiveness of the sharing model, revealing any issues or gaps in visibility that might not be apparent through reports or theoretical assessments. It helps to identify any unintended consequences of changes and confirm that users have the correct access to records based on their assigned roles and profiles. The other options—while they may provide useful information—do not deliver the same level of insight. For example, viewing Active Users reports does not show data visibility; it only shows user activity. Checking field meta-data with Field Audit Trail focuses more on the configuration of fields rather than their sharing settings. Testing through the Sharing button relates more closely to sharing rules rather than a comprehensive view of access permissions across different users. Therefore, the Login As feature is a best practice for validating user access effectively.

9. **What step should an Architect take to ensure the Director of Support has access to all Reimbursement records?**

   A. **Leave the Reimbursement Object in "Deployed" Status and set the Director of Supports Profile to "View All" in the object permissions**

   B. **Use an Approval Process to change the owner of the Reimbursement record upon submission to the Director of Support**

   C. **Disable Grant Access Using Hierarchies for the Object and create a Sharing Rule to enable sharing to the Director of Support**

   D. **Implement a public group that includes the Director of Support**

**To ensure that the Director of Support has access to all Reimbursement records, the most effective step is to disable Grant Access Using Hierarchies for the Object and create a Sharing Rule to enable sharing to the Director of Support. Disabling Grant Access Using Hierarchies means that the standard access model where users at higher levels in the role hierarchy automatically gain access to the records of lower-level users is turned off. This is important in scenarios where it is necessary to have more granular control over record visibility, ensuring that all records are only shared according to specified rules rather than through hierarchy. Creating a Sharing Rule explicitly allows access to the Director of Support for all Reimbursement records, which ensures that they can view and manage those records regardless of the record owner or their position in the hierarchy. Sharing Rules can be set up based on criteria such as roles, public groups, or various field values, making it a flexible and efficient way to grant access as needed. This strategic combination of disabling hierarchy-based access and using specific sharing rules is optimal for ensuring complete and controlled access to the desired records, aligning with Salesforce best practices around data sharing and visibility.**

## 10. How can an architect ensure object-level security is enforced in a Visualforce Application that uses a custom Apex Controller?

**A. Utilize the "With Sharing" keyword when defining the Visualforce Page**

**B. Use the Schema.DescribeSObjectResult isAccessible() method in the Apex Controller**

**C. Utilize the "Without Sharing" keyword when defining the Apex Controller Class**

**D. Use the "With Sharing" keyword when defining the Apex Controller Class**

**In the context of enforcing object-level security in a Visualforce application that employs a custom Apex controller, selecting the method that checks access permissions directly is crucial. Using the Schema.DescribeSObjectResult isAccessible() method in the Apex controller serves this purpose effectively. This method can confirm whether the current user has permission to view a specific object, thus ensuring that the application adheres to the visibility and sharing rules defined in Salesforce. By employing this method, the architect can programmatically verify access permissions before executing logic that interacts with the object. This approach not only reinforces security measures at the object level but also allows for dynamic checks based on the current user's permissions. While other options may relate to the handling of security and permissions: - The use of the "With Sharing" keyword in the Apex class enforces sharing rules for records, but it does not directly address object-level security. - Defining the Visualforce page with "With Sharing" or "Without Sharing" does not impact object-level security checks; it deals more with record-level visibility. - Using "Without Sharing" explicitly allows bypassing sharing rules, which is contrary to the intent of enforcing security. Consequently, using Schema.DescribeSObjectResult isAccessible() in the Apex controller represents a**

# 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://salesforce-sharingandvisibility.examzify.com**

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