

## Browse the Book

*This sample chapter provides an overview of different role types and how to use them. It starts by covering the different role design approaches, then dives into more detailed explanations of each role type and how they can be used in different scenarios. Next, it covers how to use segregation of duties (SoD) to separate critical functions of business processes among different roles. The chapter closes with best practices for developing a standard role naming convention.*

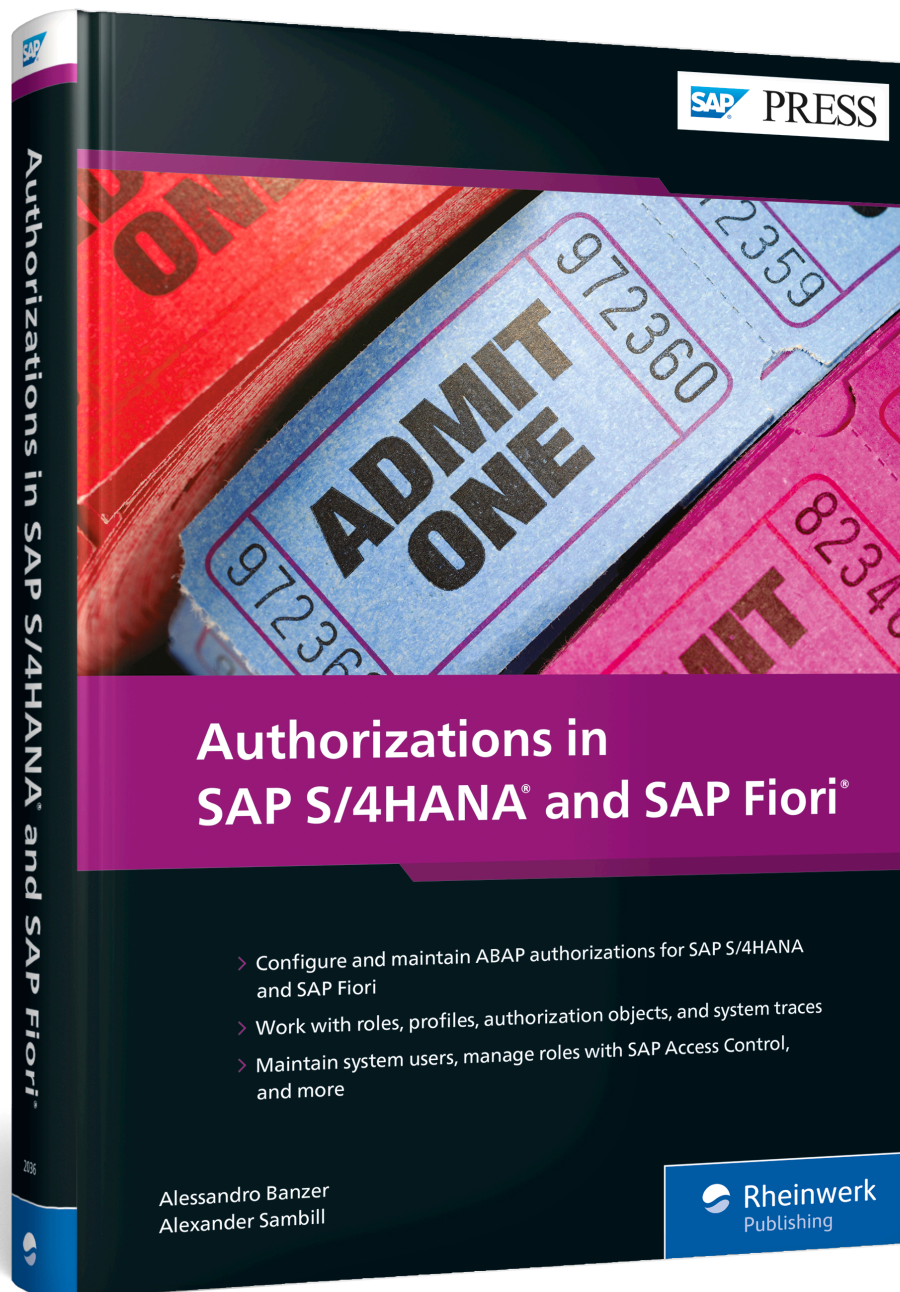
-  **“Designing Authorization Concepts”**
-  **Contents**
-  **Index**
-  **The Authors**

Alessandro Banzer, Alexander Sambill

### Authorizations in SAP S/4HANA and SAP Fiori

625 pages, 2022, \$89.95  
ISBN 978-1-4932-2036-6

 [www.sap-press.com/5203](http://www.sap-press.com/5203)



## Chapter 3

# Designing Authorization Concepts

*Designing authorization concepts is an ambitious task that requires thorough planning and deep understanding of the technical components of an authorization concept. You'll also need to understand fully how your organization runs its processes.*

This chapter provides an overview of different role design concepts and approaches, including why to favor some over others and how to use them in practice. The overall goal of a role concept is to help establish maximum security, provide sufficient authorizations for end users to fulfill their job duties, simplify user maintenance, and help you sustainably maintain your roles.

Designing an authorization concept is a complex task with multiple drivers that must be taken into account. First and foremost, you must ensure that your end users can do their jobs and run the business, but at the same time, you'll need to adhere to access governance and compliance laws and regulations. The pitfalls of a poorly designed authorization concept include loss of productivity, high maintenance effort, exposed risk for the organization, failure in audits, inefficient access provisioning, and many more. Therefore, properly thinking through a concept that is sustainable, maintainable, transparent, and upgradable in the future is vital.

Ideally, your company discusses and addresses security considerations before an actual implementation. However, more often, companies have not proactively addressed security design beforehand and are thus challenged with costly role redesign projects shortly after go-live. All too frequently, companies change, expand, and merge with or acquire other companies, thus resulting in changes to the security design. A solid and sustainable design must be flexible enough to adjust to these changes.

### 3.1 Role Design Approaches

For various reasons, as shown in Figure 3.1, a company may consider (re)designing its authorization concept. The main drivers are system upgrades (e.g., migration to SAP S/4HANA); remediation of compliance issues, such as segregation of duties (SoD) or legal requirements; mergers and acquisitions that lead to integration projects; or simply because the current design is not maintainable and access governance cannot be ensured.

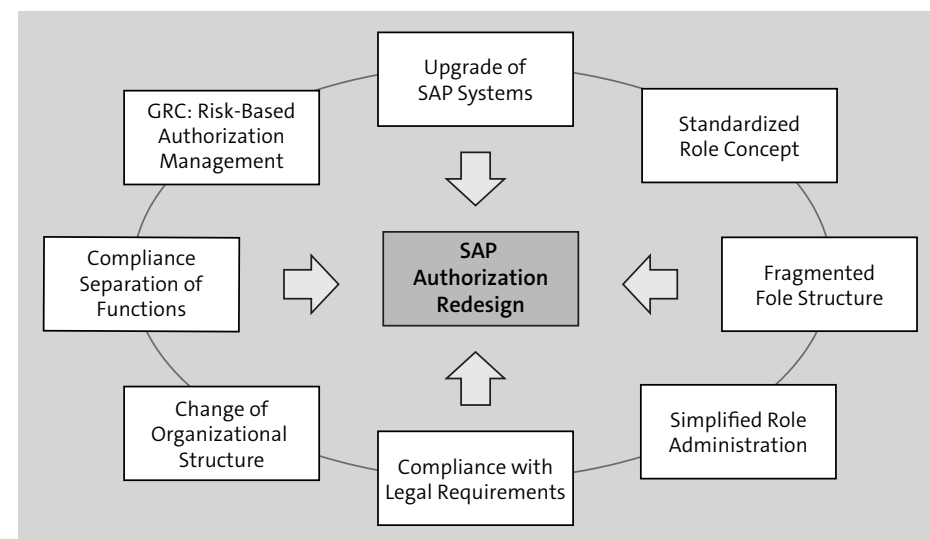


Figure 3.1 Reason for Authorization Redesign

Figure 3.2 shows some important trends regarding role design.

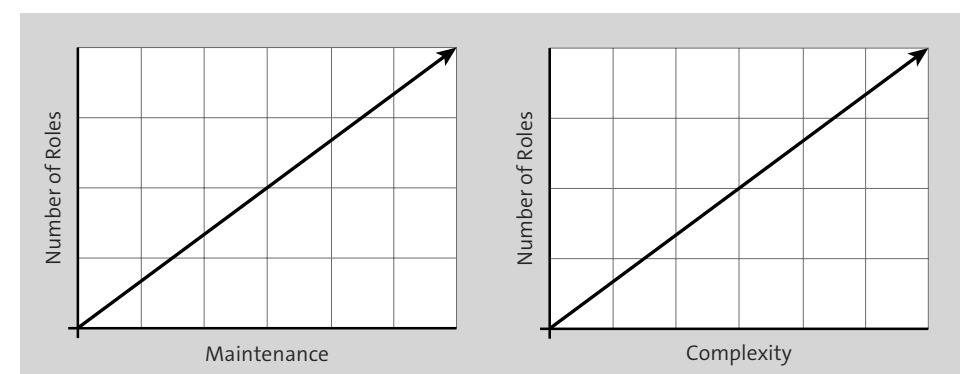


Figure 3.2 Role Design Complexity and Maintenance Effort

Regardless of the approach taken, your role concept should be as simple as possible to ensure that the investment is sustainable and long term. The number of roles should (if possible) be kept small and specific so that maintenance overhead is reduced. Complexity can be reduced when utilizing function-related (job-related) single roles. This approach increases flexibility and transparency for future adjustments of business processes, especially when considering a risk approach due to SoD or other compliance regulations.

Implementing an authorization concept can be performed in multiple ways. Two main approaches exist for building an authorization concept, but a hybrid of the two approaches can also be adopted. The first approach is the “top-down” approach, which

is a proactive way to design and conceptualize the necessary authorizations upfront, based on an analysis of business processes and job functions. With the “bottom-up” approach, the analysis starts with the available statistical usage data as well as with existing authorizations and their assignments.

Both approaches have their pros and cons. The “top-down” approach helps address security risks and requirements during the blueprinting phase but might prove to be difficult to implement. This approach requires a deep knowledge of the business processes, laws and regulations, and security implications like financial and audit requirements. The “bottom-up” approach is particularly difficult when remediating SoD conflicts, which requires inputs and an understanding of the business processes performed by business process managers. Without this knowledge, this approach tends to lead to a high number of roles built specifically to remediate SoD conflicts, which can lead to difficulty in provisioning as well as negatively impact the maintainability and sustainability of the authorization concept. This potential issue stems from the fact that, in most cases, SoD conflicts are avoided on the role level, which requires a separation of each job function.

Let’s now briefly summarize the two approaches:

■ **Top-down approach**

Information will be acquired by interviews and an analysis of the business processes performed in your organization:

- Analysis of business processes
- Jobs within processes
- Core activities
- User groups

■ **Bottom-up approach**

Information will be acquired by an analysis of the current system and its user history data:

- Existing authorizations
- Existing role assignments and users
- Use of transactions and other menu objects
- Existing organizational restrictions in the system

To further highlight the difference between the bottom-up and top-down approaches, to summarize, the bottom-up approach uses existing data (transaction usage, current role and authorization assignments, etc.) to drive the role design. In contrast, the top-down approach utilizes business processes to shape the role design. Regardless of the approach, defining security requirements early in the project is important as being proactive helps ensure efficiency during implementation. In addition, we recommend leveraging tools like SAP Access Control or similar solutions, to analyze and monitor role design to address potential SoD violations early on.

Combining both approaches allows for the best results when redesigning authorization concepts, as shown in Figure 3.3. You can take usage data and existing authorizations from the “bottom-up” approach and use that information to come up with a draft design. That draft can then be discussed with business process managers to separate out functions and fine-tune the design based on how your company runs its processes.

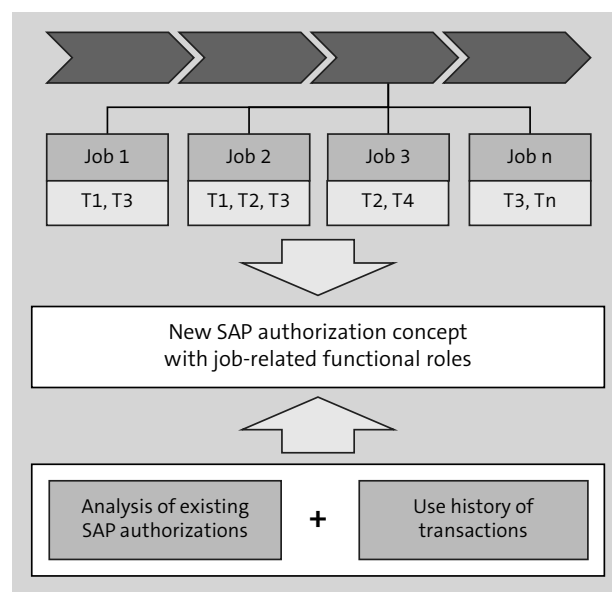


Figure 3.3 Top-Down and Bottom-Up Approaches

Before beginning the work of creating roles as part of your effort to enhance security in your SAP systems, an important decision must be made. You must decide between using *job-based roles* or *task-based roles*, and this choice will impact how your roles will be designed.

Let’s briefly look at these two concepts next:

#### ■ Job-based roles

Job-based roles are designed for including all of a person’s job activities into one single role. For instance, a person with the position of a “sales order specialist” must perform certain activities such as creating, changing, and displaying sales orders. A role encompassing all those activities for that position is an example of a job-based role design. Utilizing this role design method uses fewer roles by consolidating job duties into one role instead of creating a role for each individual job task. Be mindful, however, that this approach can be prone to SoD conflicts due to the broader access subsumed under one role. While utilizing this method, make sure you put effort into mitigating these conflicts.

Using the top-down approach “to create your job-based roles, you first must analyze business processes and their jobs-related tasks. This analysis helps outline of how

the job-based role should look. Then, you’ll move on to identifying the core activities within those jobs. This step assists with discovering the relevant transactions for the job-based role. Finally, you’ll map out your user groups to help you assign users with the right role assignments. Knowing how users are grouped together (i.e., a department) allows for efficient job role assignments through user groups.

#### ■ Task-based roles

In a task-based role design, a role is created for each job task within a job function. Continuing our earlier “sales order specialist” example, this position requires several tasks such as creating, changing, and displaying sales orders. In a task-based role design approach, a separate role will be created for each of the job task: One role will be designed for creating sales orders; another role, for changing sales orders; and the final role, for displaying sales orders—for a total of three roles. As a result, more roles are required in a task-based role in comparison to a job-based design where the role count would be one. SoD conflicts still need to be considered, but they may be reduced (on a role level) since access is more granular in these roles.

Using the bottom-up approach “to create your task-based roles, you would first analyze existing authorizations. Being knowledgeable on existing authorizations allows you to gauge existing access levels. Combining this information with the next step while reviewing existing user role assignments, you can tailor appropriate access to users based on the tasks performed in their business functions. Finally, analyzing the use of transactions helps you select which tasks should be included a task-based role. Understanding how transactions correlate to the tasks helps you properly build roles for different areas of your business.

## 3.2 Role Types

From a technical point of view, only two types of roles are available in SAP—single roles and composite roles. Single roles can further be divided into child roles that only differ from the parent role on the organizational level. However, many organizations have additional “types” of roles, for example, enabler/value roles, which technically are still single roles but have distinct intentions.

### 3.2.1 Single Roles

A single role contains all the necessary authorization objects and field values (organizational and non-organizational) required for the transactions that the role contains. In SAP, many authorization objects are represented by two types of authorization fields: the activity field and the organization value field. Technically, you cannot separate these two fields because the kernel evaluates them together during an authority check, and thus, both fields must be defined in the same role.



**Hint**

See Chapter 2, Section 2 for more information about the cumulative aspect of SAP authorizations.

However, a single role can have multiple individual authorization instances to represent different combinations of field values when these values cannot be merged into one authorization instance to be evaluated by the system check. Thus, a single role can also be a composite of authorization instances.

Typically, when someone talks about the single role concept, they are referring to a job-/position-based role design. In such cases, the role contains all the required authorizations for a user's job/position in a single role. A user might, however, have more than one job/position, such as a purchaser and a contract manager. Each role has authorizations to complete the transactions that are contained in each of the two single roles so that they are functional on their own. With this approach, no dependencies exist.

However, many "single role" designs won't contain all of a user's required authorizations. Some employees might have additional authorizations to execute special tasks. As a result, such employees may get an "additional access" single role assigned to them, for instance, with the ability to close accounting periods or approve purchase requisitions. Figure 3.4 shows an example concept of functional roles. Likewise, a common practice, as shown in Table 3.1, is to create a "basic authorization" role that contains transactions and authorizations that are common for all users, for example, the ability to print or to access office mailboxes in SAP.

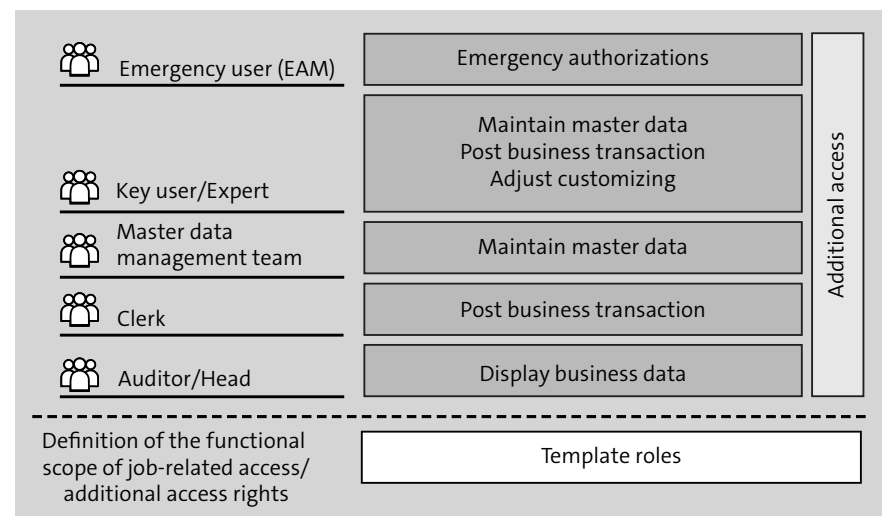


Figure 3.4 Concept of Functional Roles

Types of Role	Subtypes	Explanation
Single Roles	Template roles (Layer 00)	The role is used in the project (design phase) as a template (master role) for all singles role to be created.
	Function-related (job) roles (Layer 01-05)	Terms for the creation of functions or job profiles within the business processes such as accountants, buyers, sellers, Basis administrators, SAP developers, etc.
	Special roles (critical) (Layer 06)	Assigned for specific use or critical authorizations (such as SoD, SFX, FDA, DSG) and are targeted at specific users.
	Special roles for controlling (Layer 06)	This is only used if the requirement is to make restrictions in the area of controlling, such as cost centers, orders, profit centers, etc.
Composite Roles	Function-related roles	Terms for the summary of the function-specific roles and special roles (such as accountants, buyers, Basis staff, etc.

Table 3.1 Types of Roles and Subtypes

Likewise, you can also use single roles for role derivation. Derived roles consist of a master or parent role and additional child roles that differ from the master and from each other only in their organizational values. Please note that limitations exist with this approach. If you try to promote non-organizational fields to organizational fields, then, in this case, the values must all be the same within one role, regardless of which authorization object is using the field. In other words, you should not use different non-organizational fields in combination with derived roles because the values across all child roles will always be the same as the master role and will affect all objects.

**Hint**

Chapter 2, Section 2.3.5, contains extensive information about promoting non-organizational authorization fields.

**3.2.2 Composite Roles**

A composite role is a collection of single roles grouped together into a common composite role menu. As a result, you can indirectly assign multiple single roles to a user by assigning a composite role that contains single roles. However, you may be tempted to build numerous smaller single roles without considering the required user assignments.

Many businesses using SAP leverage composite roles to reduce the number of direct single role assignments to users. However, this approach often leads to less transparency, higher effort for maintaining more roles, and an increased risk of accidental inheritance of incorrect authorizations from a single role impacting multiple composites. The ability to change single roles rapidly leads to the side effect of having more single roles to maintain.

Technically, a composite role is a bundle of single roles to map a task-level single role (in the worst case, a transaction-level single role) to a broader role. The goal of a composite role is often to simplify the assignment of roles to users since composite roles often represent a job function. In addition to the number of single roles that may result, your organizational structure and its changes can also play a role in the choice of approach.

### 3.2.3 Enabler Roles

In recent years, we've seen role concepts in which the SAP standard has not been followed. These concepts are often called *enabler role concepts* or *value role concepts*. In these concepts, you would separate organizational authorization values from functional authorizations, which results in the need for two roles to execute a transaction successfully.

In these authorization concepts, a functional role contains all the authorization objects and values, but not the organizational level. A second, also required, enabler role contains the "missing" organizational values and enlarges a user's authorizations. Thus, to successfully execute a transaction, a user requires both the functional role and its corresponding enabler role.

The idea behind enabler roles lies in the desire to isolate organizational fields and simplify user assignments when it comes to purely organizational, non-functional distinctions.

However, any organizational type of field, which also has an "activity" field in the same authorization object, cannot be separated into a different role. This limitation is almost always the case in SAP authorization objects. Due to this absolute disadvantage, enabler roles sometimes cannot work as designed, which typically results in a proliferation of authorizations in enabler roles and the number of enabler roles, which often exceeds the number of users.

The enabler role concept sometimes looks tempting on paper, and some businesses might expect enabler roles to behave similarly to organizational management in SAP ERP Human Capital Management (SAP ERP HCM). However, you cannot apply it to authorization objects and role-based authorization concepts nor to the modern menu-based visibility access concepts, such as SAP Fiori applications and SAP Enterprise Portal/SAP Business Warehouse (SAP BW) reporting.

In addition to enabler roles for organizational values, subsets of your authorization concept can benefit from implementing enablers, for example, to restrict access to controlling scenarios or to implement a release strategy for purchase orders.

In purchasing, for example, a release strategy for purchase orders is defined, which means that purchase orders released through Transaction ME24(N) require specific authorizations. The release strategy might define the required approval level based on the purchase order amount. A user who wants to approve a purchase order requires the correct release code and release group authorizations through authorization object M\_EINK\_FRG. Since approval limits are sometimes not directly related to a job function, the release strategy is often defined in enabler roles that are individually assigned to users.

Enabler roles are special roles that can be valuable for maintaining a sustainable role concept while reducing the complexity that comes with including these special authorizations in job roles. For more information on how to determine when to use or not use an enabler role, see Section 3.4.

### 3.2.4 Authorization Templates and Standard Roles

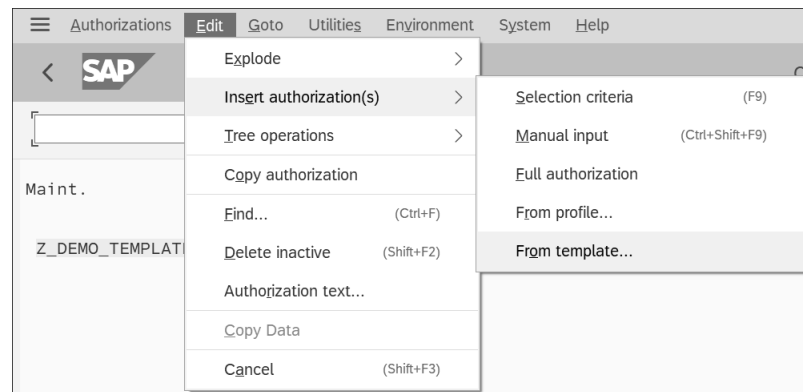
SAP standard roles and authorization templates can serve as reference points for role creation so that you don't have to start from scratch when creating roles. SAP provides standard roles and authorization templates to find business authorizations and transactions that may be relevant to your business. Using these templates and roles as starting points can save time in terms of the research effort to identify authorizations and transactions for a particular role. Template roles usually have a wide coverage of authorizations, so they should be used as a reference to tailor roles to your business needs. For instance, the authorization template SAP\_AIF\_USER is for personnel responsible for error handling and monitoring interfaces. This template comes with a set of authorizations and transactions, such as editing fields, restarting, and canceling data messages. However, you must keep in mind that templates are valuable in sandbox and testing environments, but should be avoided in productive landscapes. Authorization templates are manually added authorizations that are far reaching. SAP standard roles are also far reaching, and the roles are routinely updated by SAP. As a result, during the next system upgrade, SAP-delivered roles are overwritten. Therefore, you should never use standard roles or standard authorization templates directly in your productive landscape as assignments to your end users. Standard templates and roles from SAP should only serve as reference points for building your own distinct custom roles.

To add authorizations from a template, follow these steps:

1. Go to Transaction PFCG.
2. Enter your role name and click on the kind of role you want to create (**Single** or **Composite**). In this example, we are creating a single role.

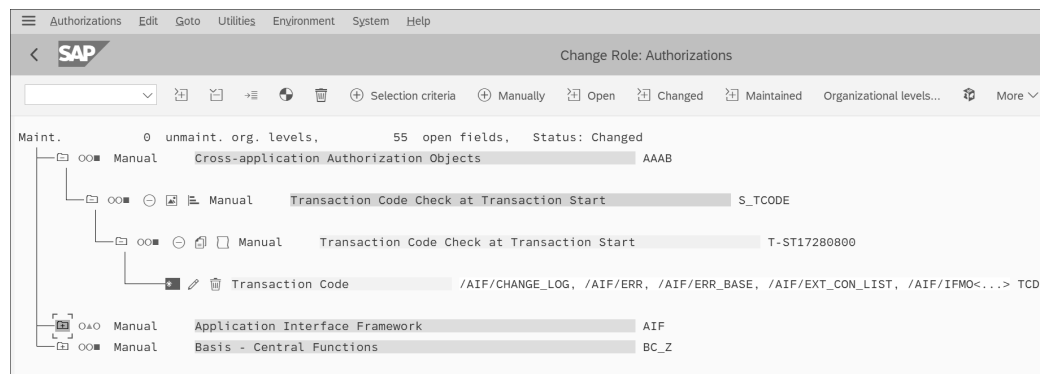
3. Go to the **Authorizations** tab.
4. Click on the icon next to **Expert Mode** for **Profile Generation**.
5. As shown in Figure 3.5, follow the menu path **Edit • Insert authorization(s) • From template....**

Using templates as a starting point, you can then tailor transactions and authorizations as needed for your company.



**Figure 3.5** Inserting Authorizations from a Template

Please keep in mind that inserting authorizations from a template adds all the authorizations as manual objects, as shown in Figure 3.6. This approach goes against best practices but is helpful when trying to understand what authorizations are required. To properly authorize your roles, you should add the transactions through your role menu so that you can leverage authorization proposals from Transaction SU24.



**Figure 3.6** Manually Inserted Authorizations from a Template

In addition to using templates as a reference, you can also refer to SAP-delivered standard roles that are available in Transaction PFCG. SAP standard roles start with the prefix “SAP\_”.

### 3.2.5 Comparison of the Role Design Concepts

Table 3.2 provides a detailed overview of the pros and cons of the various role design concepts and is a product of years of experience and best practices. Earlier, Figure 3.4 showed a proposed model for building your own roles.

Requirements	Enabler Roles	Single Roles (with Optional Derivation)	Composite Roles
Effort of initial role definition	Well supported	Well supported	Partially supported
Possibility to optimize grouping of applications	Partially supported	Well supported	Partially supported
Possibility to individualize role assignments	Not supported	Well supported	Partially supported
Reduction of Functional/organizational redundancies	Partially supported	Well supported	Partially supported
Effort of functional role maintenance	Not supported	Well supported	Not supported
Effort of organizational role maintenance	Partially supported	Partially supported	Partially supported
Effort of user assignment maintenance	Not supported	Partially supported	Partially supported
Compliance in data protection at role level	Well supported	Well supported	Well supported
Compliance with SoD at the role level	Partially supported	Well supported	Well supported
Possibility of role mining	Partially supported	Partially supported	Not supported
Cascading of SAP role design	N/A	Well supported	Not supported
Reporting (auditing, transparency)	Not supported	Well supported	Partially supported

**Table 3.2** Comparison of Different Role Designs

Requirements	Enabler Roles	Single Roles (with Optional Derivation)	Composite Roles
Upgrade capability (e.g., enhancement packages [EHPs], SAP S/4HANA)	Not supported	Well supported	Well supported
Maintenance after role creation	Not supported	Well supported	Not supported

**Table 3.2** Comparison of Different Role Designs (Cont.)

As shown in Table 3.2, building single roles (with optional derivation) is considered a best practice for SAP role designs. This approach offers the greatest flexibility, transparency, and the broadest support in terms of requirements and upgrades. On the other side of the spectrum, you might use enabler roles, which are the least flexible and have several design and maintenance disadvantages.

### 3.3 Segregation of Duties

No matter the approach you choose, you should always consider SoD during your role design. SoD is an internal risk management control used to separate critical functions of a business process among different individuals. SoD is an effort to lessen risks and fraud by preventing one individual from having too much authorization within a business process. A good demonstration of SoD would be separating the responsibilities of creating a purchase order and the receiving of goods to two different individuals. Leaving both purchasing tasks to one person can lead to increased risk of fraud because no control is in place to prevent an individual from engaging in fraud.

Keeping SoD in consideration during role design helps improve security by reducing the area where risks can occur and be exploited. Depending on your company's architecture, modeling the design of your SoD process can be time consuming and cumbersome. Thus, be mindful when creating your SoD policies and risk levels. SoD risk levels help your business prioritize risk mitigation. An example of risk levels could be critical, high, medium, or low. A critical risk in most cases would be prioritized over a medium- or low-level risk. This classification scheme helps a business control how and when risks are dealt with. Knowing the organizational risks and SoD rules can help you calculate the number of roles that need to be created when segregating access on a role level, as shown in Table 3.3. Regardless of which role design approach you choose, SoD should be an integral component of your role design process.

Number of Risks	Number of SoD Functions	Number of Organizations (Departments)	Calculation of Number of Single Roles
20	15 to 30	10 company codes	15 × 10 = 150 30 × 10 = 300
50	40 to 75	10 company codes	40 × 10 = 400 75 × 10 = 750

**Table 3.3** Role Calculation Based on SoD

A few key aspects to keep in mind when considering SoD in your role concept include the following:

- Keep risks low. Discuss the necessity of specific risks with your internal and external auditors. More risk leads to more separation, and thus, more roles are required.
- Define the criticality of the specific risks by using risk levels (critical, high, medium, low, etc.). This approach helps you prioritize risks.
- Encapsulate SoD functions in separate roles only when risks have been defined with the highest criticality.
- Encapsulate SoD functions in separate roles only when risks have no defined mitigation. If mitigations and compensating controls are available, mitigate the risk rather than split on the role level.
- Encapsulate SoD functions in separate roles only when a functional separation is possible and can be implemented in the future organizational and procedural framework.

SoD can have a huge influence on role design, and you must determine on which level the separation should take place. At the end of the day, SoD conflicts matter on the user level but must be separated on the role level in order to fully remediate. However, depending on the risk and whether mitigations are available, SoD conflicts should be managed on the role level.

### 3.4 Determining When to Use Enabler Roles

The enabler role concept is a non-standard approach to role design. Its origins are based on the assumption that you cannot create a role that can display all items but only change a subset. Technically, this impossibility is because an authorization object with two or more fields will check all of them and require that they are present in the same role authorization.



The following section describes a simple example of an enabler role for Transaction FK03 (Display Vendors). The single role contains the transaction (a transactional single role), and another single role contains the organizational values (the enabler role).

The transactional single role contains Transaction FK03 with all its authorization objects and values, as shown in Figure 3.7. The organizational level (**BUKRS** in this example) for object **F\_LFA1\_BUK** is left empty, or the authorization object is deactivated.

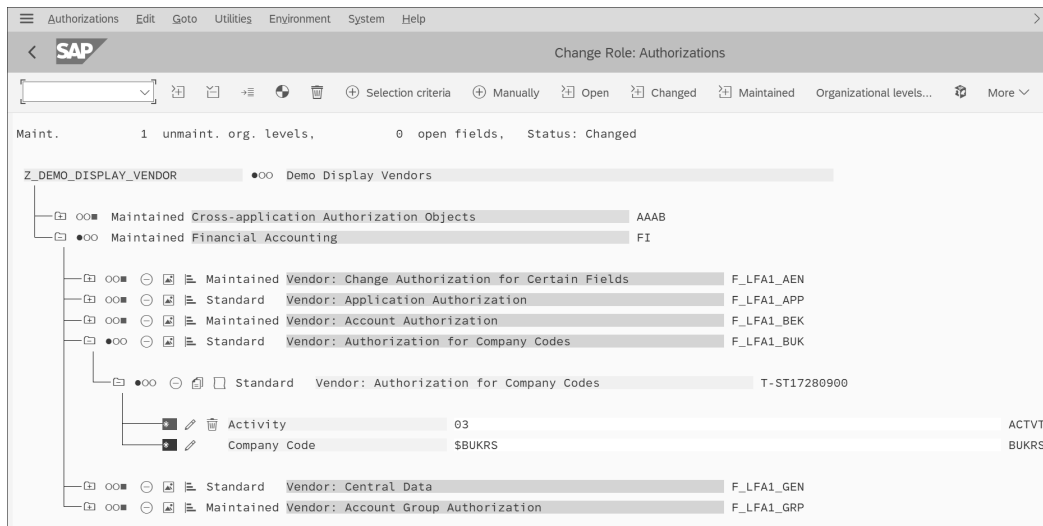


Figure 3.7 Example of the Transactional Role for Transaction FK03

A second role, the enabler role, contains the organizational values for authorization object **F\_LFA1\_BUK** only, as shown in Figure 3.8. No other authorizations—other than the objects with organizational values—are maintained in this enabler role.

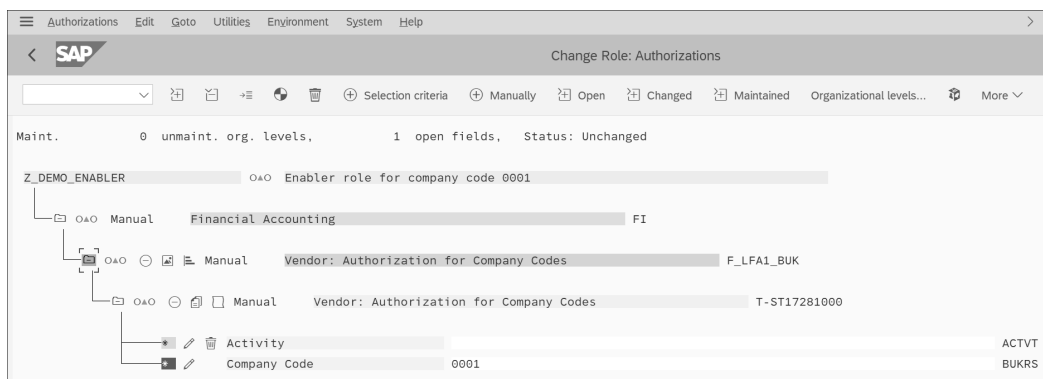


Figure 3.8 Enabler Role Containing Object F\_LFA1\_BUK

When the two roles are assigned to a user, you can check the user buffer to see the totality of assigned authorizations. In the user buffer (Transaction SU56), shown in Figure 3.9, you'll see the two authorization profiles assigned to the user, with two instances of the authorization object **F\_LFA1\_BUK**. Notice how the **ACTVT** value **03** comes from the transactional single role, but the company code comes from the enabler role.

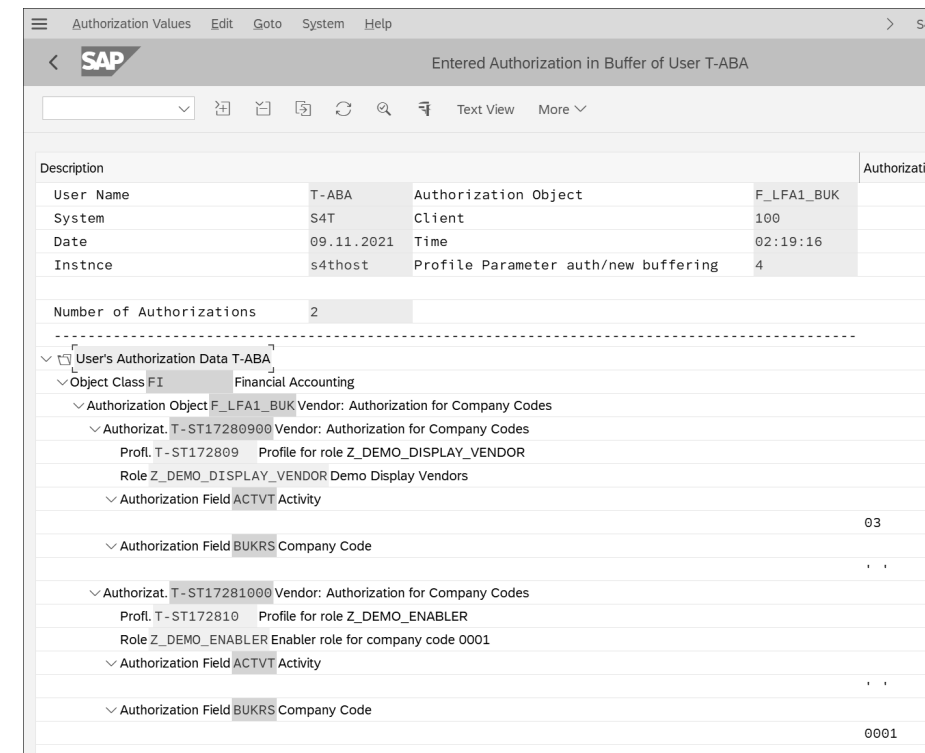
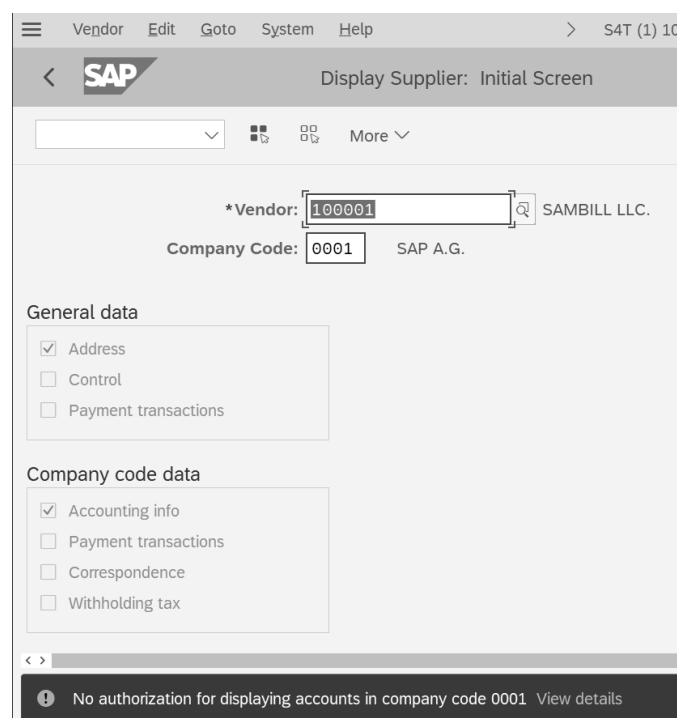


Figure 3.9 User Buffer of User with Both Roles Assigned

Since the two authorizations are in different authorization profiles, the authorization check does not succeed. This failure is because, when the kernel performs an authority check, it checks the values of one authorization instance. As shown in Figure 3.10, the user can still successfully launch Transaction FK03 but is missing the authorization for company code 0001.

At this point, the user can successfully execute the transaction but cannot view vendors in company code 0001, even though the enabler role contains the company code. Since the kernel checks the activity and the company code in the same authorization instance, the authorization check was unsuccessful. Therefore, you cannot have activity in one role and the organizational field in another and expect that the check will be successful as a whole.



**Figure 3.10** Authorization Error while Accessing Company Code 0001 in Transaction FK03

To counter this issue, you must authorize your enabler roles with the activity fields that control the company code. In this particular case, you must ensure that authorization object F\_LFA1\_BUK is restricted to display access (**ACTVT = 03**) because, otherwise, you'll overauthorize these users. This potential issue is a main concern when using enabler roles since your enablers tend to carry far-reaching authorizations that may cause critical access and SoD conflicts.

Another downside to this approach is the fact that, in typical enabler concepts, the enabler roles contain almost every authorization object that has organizational fields. Since many critical business authorization objects within SAP contain organizational fields, often all these fields are added to the enabler role, since the goal of the enabler concept is to keep the number of enablers low.

In addition to this complexity, enabler role designs can also lead to several other issues, such as the following:

- You're breaking with the SAP standard. Transaction SU24 is used to propose required authorization objects into Transaction PFCG. Breaking this standard and manually inserting objects will impact upgrades, security patches, complexity, where-used list reporting, and more.

- You must use manually inserted objects with enabler roles instead of relying on solid Transaction SU24 proposals for the activity type of fields. As a result, authorization objects and values in the role profiler are not related to an application. You cannot use the where-used list to see why the authorization object was added in the first place. Over time, as role requirements change, typically obsolete authorization values become a mess that no longer matches their original intention to "enable" the transaction.
- Maintenance of roles after creation is typically more labor intensive than a derived role design due to the lack of automation. The number of enabler roles can explode such that there are more roles than there are users in the system.
- You cannot run SoD analysis on the role level with governance, risk, and compliance (GRC) tools like SAP Access Control or check on S\_TCODE and the related authorizations of other objects. If transactions, activities, and organizational authorization objects are separated, you would need to simulate the correct pairing of roles to have the full set of authorizations to be assigned to a user. Please note that SoD conflicts matter the most when assigned to a user. At this point, enabler role concepts are tempted to use composite roles for role assignments, in this way adding the additional disadvantages of composite roles on top of enabler roles.
- Enabler role designs increase the complexity of role mining during the user provisioning process. For a requestor who has to request access, finding two roles is significantly harder than finding one. Especially when using tools like SAP Identity Management (SAP ID Management) or SAP Access Control, a requestor must both understand the concept as well as identify and find matching pairs of roles.
- Role testing becomes exponentially more complex since you'll need to test pairs of roles. This effort continues to be required as an organizational structure changes and roles must be tested again to ensure they reflect these changes.

Most of these issues arise because of missing Transaction SU24 content for what the application needs. Over time and by necessity, manually inserted authorization objects become obsolete, become incorrect, and overauthorize users. Since manually inserted objects are not attached to a transaction, no easy way exists to identify to which transaction they belong and why they were added to the enabler role in the first place. In the long run, maintaining and upgrading these roles is a nightmare.

If composite roles are additionally used for user assignments, then a cascading problem occurs, and changing an enabler role is nearly impossible—thus, administrators typically must create more new enabler roles to compensate.

### 3.5 Role Naming Convention

Before you start building your roles, we recommend spending some time developing a role naming convention that suits your organization. A common mistake is building roles without any convention, thus resulting in a messy design that is hard to maintain in the long run. Also, the lack of naming convention increases the complexity of finding and assigning roles to end users. Especially when companies use tools such as SAP ID Management or SAP Access Control for role provisioning through workflows where a requester has to enter the roles that shall be assigned to a user.

Table 3.4 is an example of a role naming convention that has been implemented successfully with many clients.

Character Number	Description	Examples
1	Fixed value "Z" for customer namespace	
2	Identifier for the system level	P – Production D – Development T – Test S – Sandbox Q – Quality I – Integration
3	Fixed character "_" for separation	
4	Identifier for role type	S – Single role C – Composite role M – Master role
5	Identifier for user group	C – "Common" role for basic functions for all users E – end user role for job function I – IT roles for administrators, developers, etc. T – Technical roles for remote function calls (RFC), batch jobs, Web Services, etc. R – Reference user roles
6	Fixed character "_" for separation	

Table 3.4 Example of a Role Naming Convention

Character Number	Description	Examples
7 – 8	Identifier for business area	BC – Basis BI – Business Intelligence CR – Customer Relations CO – Controlling EC – ERP Component FI – Finance HR – Human Resource MM – Material Management PI – Process Integration PS – Project Systems SD – Sales & Distribution SM – Solution Manager SR – Supplier Relations
9	Fixed character "_" for separation	
10	Identifier for leading organizational element	A – All N – None C – Company Code P – Purchasing organization P – Plant D – Division
11	Fixed character "_" for separation	
12 – 15	Organizational value in regard to the organizational element	A – GLOB (all) N – GLOB (none) C – \$BUKRS (value from company code) S – \$VKORG (value from sales organization) P – \$WERKS (value from plant)
16	Fixed character "_" for separation	

Table 3.4 Example of a Role Naming Convention (Cont.)

Character Number	Description	Examples
17 – 19	Identifier for activity group in regard to the user group	COM – Common job authorizations REP – Reporting with display only authorization EAM – emergency access authorizations KEY – Key user authorizations MDM – master data authorization ADM – administration authorization HPU – High-privileged user (HPU) authorizations
20	Fixed character “_” for separation	
21+	Free text	

**Table 3.4** Example of a Role Naming Convention (Cont.)

Based on the role naming convention in Table 3.4, a few practical examples might resemble the following role names:

- **ZP\_SI\_BC\_N\_GLOB\_HPU\_OPEN\_CLIENT**  
A single role for a productive system (PRD) that does not include any organizational data and is considered an HPU role to open clients.
- **ZP\_CE\_FI\_C\_1000\_REP\_ACCOUNTANT**  
A composite role for a PRD that includes organizational values for company code 100 with display-only access for reporting purposes, typical for an accountant.

With this kind of role naming convention, not only can an administrator easily understand a number of roles, so can an end user. Also, since identifiers are defined and follow a specific pattern, role analysis can be simplified. For example, a role that contains “REP” in characters 17 to 19 is a reporting-only role that should not include any insert, change, update, or delete authorizations. For role quality and sustainability purposes, a strictly enforced role naming convention is therefore mandatory.

### 3.6 Summary

The decision to (re)design a company’s authorization concept can be stem from a variety of reasons. Some main drivers include system upgrades (e.g., migration to SAP S/4HANA); remediating compliance issues (e.g., SoD, legal requirements); mergers and acquisitions that lead to integration projects; or because the current design does not meet the desired security standards of your company. When choosing between the types of approaches (top-down or bottom-up), be mindful of how each can affect your

authorization concept design. Additionally, some areas to take note of when designing your company’s authorization concept include the following:

- Existing SoD policies
- Role naming conventions
- Job- or task-based roles
- Knowing when to use single, derived, composite, enabler, or template roles

In the next chapter, we’ll discuss the Xiting Authorizations Management Suite (XAMS).



# Contents

Preface .....	19
<b>1 Introduction to SAP Authorizations</b> .....	<b>23</b>
1.1 What Are Authorizations? .....	24
1.2 User Access in the SAP System .....	25
1.3 Evolution of Authorizations from SAP ERP to SAP S/4HANA .....	26
1.3.1 SAP ERP .....	26
1.3.2 SAP S/4HANA .....	27
1.3.3 SAP S/4HANA Deployments .....	30
1.3.4 Other SAP Cloud Solutions .....	33
1.4 SAP Fiori (Presentation Layer) .....	34
1.5 Native Authorizations in SAP HANA (Database Layer) .....	37
1.6 Hybrid System Landscapes and Implications on Authorizations .....	38
1.6.1 Business Roles and SAP Business Technology Platform .....	39
1.6.2 SAP Cloud Identity Access Governance .....	40
1.6.3 Access Provisioning in Hybrid Landscapes .....	41
1.6.4 Access Risk Analysis in Hybrid Landscapes .....	43
1.7 Summary .....	45
<b>2 ABAP Authorization Concept</b> .....	<b>47</b>
2.1 Influences on the SAP Authorization Concept .....	48
2.2 Basic Principles for an SAP Authorizations Concept .....	49
2.3 ABAP Authorizations .....	51
2.3.1 Components .....	52
2.3.2 Authorization Default Values .....	56
2.3.3 Code-Based Namespaces .....	57
2.3.4 Creating Custom Authorizations .....	58
2.3.5 Creating Custom Organizational Levels .....	61

<b>2.4 Roles and Profiles</b> .....	65
2.4.1 Roles .....	65
2.4.2 Profiles .....	67
<b>2.5 Users</b> .....	70
2.5.1 User Master Record .....	71
2.5.2 User Buffer .....	72
2.5.3 User Types and Maintenance .....	73
<b>2.6 Authority Checks</b> .....	74
2.6.1 Locking Status Checks .....	74
2.6.2 Application Start Checks .....	75
2.6.3 Transaction Start Plausibility Checks .....	76
2.6.4 Parameter Checks .....	77
2.6.5 Kernel Checks .....	78
2.6.6 Program Code Authority Checks .....	78
2.6.7 SAP System Authorization Check Processing .....	80
2.6.8 Switchable Authorizations .....	81
2.6.9 Deactivating Authorization Checks .....	85
<b>2.7 Critical Authorizations</b> .....	87
2.7.1 Critical Access Scenarios .....	88
2.7.2 Audit-Focused Authorization Objects .....	96
<b>2.8 Authorizations in SAP ERP Human Capital Management</b> .....	102
2.8.1 Business Transactions and Authorization Components .....	103
2.8.2 All-Access in SAP ERP Human Capital Management .....	105
<b>2.9 Different Transaction Types</b> .....	106
2.9.1 Overview of Available Transactions .....	107
2.9.2 Creating Custom Transactions .....	111
2.9.3 Locking and Unlocking Transactions .....	120
<b>2.10 SAP System Check for Security Flaws</b> .....	121
2.10.1 System Configuration Analysis .....	122
2.10.2 Document Analysis .....	125
2.10.3 Roles Analysis .....	125
2.10.4 User Analysis .....	128
<b>2.11 Customizing of SAP Security Settings</b> .....	130
2.11.1 Table PRGN_CUST .....	131
2.11.2 Table SSM_CUST .....	132
2.11.3 Table USR_CUST .....	133
<b>2.12 Summary</b> .....	133

<b>3 Designing Authorization Concepts</b> .....	135
<b>3.1 Role Design Approaches</b> .....	135
<b>3.2 Role Types</b> .....	139
3.2.1 Single Roles .....	139
3.2.2 Composite Roles .....	141
3.2.3 Enabler Roles .....	142
3.2.4 Authorization Templates and Standard Roles .....	143
3.2.5 Comparison of the Role Design Concepts .....	145
<b>3.3 Segregation of Duties</b> .....	146
<b>3.4 Determining When to Use Enabler Roles</b> .....	147
<b>3.5 Role Naming Convention</b> .....	152
<b>3.6 Summary</b> .....	154
<b>4 Xiting Authorizations Management Suite</b> .....	157
<b>4.1 Overview</b> .....	158
<b>4.2 Xiting Role Designer</b> .....	159
4.2.1 Capabilities .....	160
4.2.2 Analysis and Design .....	161
4.2.3 Reporting Options of Xiting Role Designer .....	162
4.2.4 Reporting Options for Menu Objects .....	163
4.2.5 Reporting Options for Business Data .....	164
<b>4.3 Xiting ABAP Alchemist</b> .....	165
<b>4.4 Xiting Role Replicator</b> .....	169
4.4.1 Bulk Processing of Users, Roles, and Authorizations .....	169
4.4.2 OrgSet Replication .....	171
<b>4.5 Xiting Role Builder</b> .....	172
<b>4.6 Xiting Times</b> .....	174
<b>4.7 Xiting Role Profiler</b> .....	176
<b>4.8 Xiting Security Architect</b> .....	179
<b>4.9 Summary</b> .....	182

<b>5</b>	<b>Transaction SU24: Authorization Default Values</b>	183
<b>5.1</b>	<b>Overview</b>	184
5.1.1	What Are SAP Authorization Default Values?	184
5.1.2	Technical Background of Authorization Default Values	187
5.1.3	Helpful Tables	190
5.1.4	System Layer Alignment	191
<b>5.2</b>	<b>Transaction SU24 Maintenance</b>	192
5.2.1	Instruments of Transaction SU24	192
5.2.2	Proposal and Check Indicator Statuses	194
5.2.3	Maintenance of Default Values and Check Indicators	195
5.2.4	Comparison between SAP Data and Customer Data	199
<b>5.3</b>	<b>Transaction SU24N</b>	200
5.3.1	General Changes	200
5.3.2	Maintaining a Description for Transaction SU24 Data	202
5.3.3	Default Data Variants	202
<b>5.4</b>	<b>Populating Data from Traces</b>	205
<b>5.5</b>	<b>Best Practice Maintenance of Transaction SU24</b>	208
5.5.1	Authorization Field Maintenance	209
5.5.2	List Navigation	214
5.5.3	Menu Navigation	216
5.5.4	Navigation Considerations	220
5.5.5	Cockpit Transactions	220
<b>5.6</b>	<b>Upgrading Authorization Default Values</b>	223
5.6.1	Importance of Upgrading	223
5.6.2	Report SU24_AUTO_REPAIR	225
5.6.3	Related Applications and Tables for a Transaction SU25 Upgrade	227
5.6.4	Performing the Upgrade for Default Values	228
5.6.5	Troubleshooting	238
<b>5.7</b>	<b>Transaction SU24 Optimization Tools</b>	239
<b>5.8</b>	<b>Xiting Authorizations Management Suite: Transaction SU24 Optimization Tools</b>	241
5.8.1	Xiting Role Profiler	241
5.8.2	Xiting ABAP Alchemist	242
5.8.3	Xiting Role Builder SU24 Checkman	242
<b>5.9</b>	<b>Summary</b>	243

<b>6</b>	<b>Role Maintenance in Transaction PFCG</b>	245
<b>6.1</b>	<b>Navigation within Transaction PFCG</b>	247
6.1.1	Initial Screen of Transaction PFCG	247
6.1.2	Single Role Maintenance Options and Tabs	248
6.1.3	Composite Role Maintenance Options and Tabs	254
<b>6.2</b>	<b>Creation of Different Roles</b>	256
6.2.1	Role Building and Naming	257
6.2.2	Single Roles	259
6.2.3	Composite Roles	259
6.2.4	Reference and Derived Roles	261
6.2.5	Customizing Roles	265
6.2.6	Role Templates	268
6.2.7	Assigning and Removing Roles via Transaction PFCG	269
<b>6.3</b>	<b>Role Menu Objects</b>	270
6.3.1	Different Maintainable Applications	270
6.3.2	Using Transaction SU24 Variants	271
6.3.3	Role Menu Comparison	273
<b>6.4</b>	<b>Authorization Maintenance in Roles</b>	274
6.4.1	Authorization Maintenance Buttons	275
6.4.2	Authorization Object Statuses	277
6.4.3	Authorization Object Update Status Texts	281
6.4.4	Maintenance of Organizational Levels	282
6.4.5	Where-Used Lists	285
6.4.6	Authorization Templates and Other Authorization Insert Options	286
6.4.7	Import of Traces to Roles	287
<b>6.5</b>	<b>Sustainable Role Building</b>	290
6.5.1	Best Practice Presettings for Role Maintenance	291
6.5.2	Best Practice Role and Authorization Maintenance	292
6.5.3	Role Profile Generation	296
<b>6.6</b>	<b>Role Versions</b>	297
<b>6.7</b>	<b>Roles Overview Status</b>	299
<b>6.8</b>	<b>Selected Mass Maintenance Options for Roles</b>	301
6.8.1	Mass Role Maintenance	301
6.8.2	Mass Generation of Role Profiles	304
6.8.3	Mass User Comparison of Roles	305
<b>6.9</b>	<b>Transfer of Roles</b>	306
<b>6.10</b>	<b>Xiting Authorizations Management Suite: Virtual Role Design with Xiting Role Designer</b>	308

6.10.1	Project Cockpit .....	309
6.10.2	Design Cockpit .....	310
6.10.3	Reports Cockpit .....	311
<b>6.11</b>	<b>Summary .....</b>	<b>312</b>
<b>7</b>	<b>Authorization Analysis, Trace Tools, and Authorization Debugging .....</b>	<b>315</b>
<b>7.1</b>	<b>Overview .....</b>	<b>316</b>
7.1.1	Analysis Tools .....	316
7.1.2	Selected Authorization Trace Return Codes .....	318
7.1.3	Activation of Profile Parameters .....	319
7.1.4	Trace Tool Use Cases .....	320
<b>7.2</b>	<b>Transaction SU53 .....</b>	<b>320</b>
7.2.1	Description .....	321
7.2.2	Authorization Check Failures Evaluation .....	322
<b>7.3</b>	<b>Transactions ST01/STAUTHTRACE .....</b>	<b>323</b>
7.3.1	Description .....	324
7.3.2	Trace Evaluation for an Authorization Error .....	326
<b>7.4</b>	<b>Transaction STUSOBTRACE .....</b>	<b>329</b>
7.4.1	Description .....	329
7.4.2	Authorization Default Value Maintenance .....	331
<b>7.5</b>	<b>Transaction STUSERTRACE .....</b>	<b>333</b>
7.5.1	Evaluation of Specific Job Functions .....	334
7.5.2	Using Transaction STSIMAUTHCHECK .....	335
<b>7.6</b>	<b>Authorization Debugging .....</b>	<b>337</b>
<b>7.7</b>	<b>Xiting Authorizations Management Suite: Enhanced Trace Evaluation .....</b>	<b>344</b>
7.7.1	Description .....	345
7.7.2	Rapidly Analyze Authorization Failure .....	346
<b>7.8</b>	<b>Summary .....</b>	<b>347</b>
<b>8</b>	<b>SAP Fiori Authorizations .....</b>	<b>349</b>
<b>8.1</b>	<b>Overview .....</b>	<b>349</b>
8.1.1	Principles of SAP Fiori .....	349
8.1.2	SAP Fiori End-User Applications .....	350

<b>8.2</b>	<b>SAP Fiori Architecture .....</b>	<b>351</b>
<b>8.3</b>	<b>Deployment Options .....</b>	<b>353</b>
8.3.1	Embedded Deployment .....	353
8.3.2	Central Hub Deployment .....	354
8.3.3	SAP Launchpad Service .....	355
<b>8.4</b>	<b>SAP Fiori Apps Reference Library .....</b>	<b>356</b>
8.4.1	Overview .....	356
8.4.2	Technical Components .....	358
<b>8.5</b>	<b>SAP Fiori Administrative Tools .....</b>	<b>360</b>
8.5.1	SAP Fiori Launchpad Designer .....	360
8.5.2	SAP Fiori Launchpad Content Manager .....	362
8.5.3	SAP Fiori Launchpad App Manager .....	363
8.5.4	Manage Spaces and Pages App .....	365
<b>8.6</b>	<b>OData Services .....</b>	<b>366</b>
8.6.1	Description .....	366
8.6.2	Activation of OData Services in Backend Servers .....	367
8.6.3	Overview of Activated Services .....	369
<b>8.7</b>	<b>SAP Fiori Concept Implementation .....</b>	<b>369</b>
8.7.1	Technical and Business Catalogs .....	370
8.7.2	Business Groups .....	374
8.7.3	Business Spaces and Pages .....	377
8.7.4	SAP Fiori Launchpad Personalization .....	378
<b>8.8</b>	<b>Frontend/Backend Server Authorizations .....</b>	<b>379</b>
8.8.1	SAP Fiori Role Concept .....	380
8.8.2	Role Building Preparation .....	382
8.8.3	Role Building for SAP Fiori Applications in the Embedded Deployment .....	385
<b>8.9</b>	<b>Troubleshooting Tools for SAP Fiori .....</b>	<b>386</b>
<b>8.10</b>	<b>Xiting Authorizations Management Suite: Tool-Driven SAP Fiori Objects Implementation and Analysis .....</b>	<b>392</b>
8.10.1	Xiting Role Replicator .....	392
8.10.2	Xiting Role Profiler .....	393
<b>8.11</b>	<b>Summary .....</b>	<b>394</b>
<b>9</b>	<b>User Maintenance .....</b>	<b>395</b>
<b>9.1</b>	<b>Maintenance of the User Master Record .....</b>	<b>395</b>
9.1.1	Different User Types .....	396



9.1.2	Creating and Maintaining a User .....	397
9.1.3	Copying a User .....	406
9.1.4	Change Documents for Users .....	406
9.1.5	Mass User Changes with Transaction SU10 .....	409
9.1.6	Inactive Users .....	415
<b>9.2</b>	<b>Password Rules .....</b>	<b>415</b>
<b>9.3</b>	<b>The User Buffer .....</b>	<b>417</b>
<b>9.4</b>	<b>User Naming Conventions .....</b>	<b>419</b>
<b>9.5</b>	<b>User Classification .....</b>	<b>421</b>
<b>9.6</b>	<b>User-Related Tables .....</b>	<b>421</b>
<b>9.7</b>	<b>User Access Reviews .....</b>	<b>422</b>
<b>9.8</b>	<b>User Lock Status .....</b>	<b>423</b>
<b>9.9</b>	<b>Security Policies .....</b>	<b>423</b>
<b>9.10</b>	<b>Securing Default Accounts .....</b>	<b>428</b>
<b>9.11</b>	<b>Maintaining User Groups .....</b>	<b>430</b>
<b>9.12</b>	<b>Central User Administration .....</b>	<b>432</b>
9.12.1	Overview .....	432
9.12.2	Distribution Parameters for Fields (Transaction SCUM) .....	433
9.12.3	Central User Administration-Related Tables .....	435
<b>9.13</b>	<b>SAP Usage Data for Users .....</b>	<b>436</b>
<b>9.14</b>	<b>Summary .....</b>	<b>437</b>
<b>10</b>	<b>Access Governance with SAP Access Control and SAP Cloud Identity Access Governance .....</b>	<b>439</b>
<b>10.1</b>	<b>SAP Access Control .....</b>	<b>439</b>
<b>10.2</b>	<b>SAP Cloud Identity Access Governance .....</b>	<b>443</b>
10.2.1	Core Functionalities .....	443
10.2.2	Key Capabilities of SAP Cloud Identity Access Governance .....	447
10.2.3	Integrated Identity Access Governance for Hybrid Landscapes .....	448
<b>10.3</b>	<b>Understanding the Ruleset .....</b>	<b>449</b>
10.3.1	Ruleset Components .....	449
10.3.2	Ruleset Architecture .....	451
10.3.3	SAP Standard Rulesets .....	452
10.3.4	Organizational Rules .....	454
10.3.5	Simulating Risk During Role Building with the Risk Terminator .....	455

<b>10.4</b>	<b>Segregation of Duties Management Process .....</b>	<b>456</b>
10.4.1	Phases of Segregation of Duties Management .....	456
10.4.2	Remediation and Mitigation of Risks .....	457
10.4.3	Continuous Segregation of Duties Monitoring .....	462
<b>10.5</b>	<b>Custom Transactions for the Ruleset .....</b>	<b>463</b>
10.5.1	Analyzing Custom Transactions .....	463
10.5.2	Enhanced Analysis with Xiting ABAP Alchemist .....	466
<b>10.6</b>	<b>Business Roles .....</b>	<b>468</b>
<b>10.7</b>	<b>User Access Review .....</b>	<b>470</b>
<b>10.8</b>	<b>Roles for Firefighters .....</b>	<b>471</b>
10.8.1	Defining Appropriate Usage .....	472
10.8.2	Firefighter Types .....	473
10.8.3	Provisioning Strategies for Firefighters .....	474
<b>10.9</b>	<b>Impact to Governance, Risk, and Compliance When Migrating and Upgrading SAP Systems .....</b>	<b>475</b>
<b>10.10</b>	<b>Summary .....</b>	<b>476</b>
<b>11</b>	<b>Interface Authorizations and Hardening of Interfaces .....</b>	<b>477</b>
<b>11.1</b>	<b>Remote Function Call Security .....</b>	<b>477</b>
11.1.1	Overview .....	478
11.1.2	Trusted and Untrusted Remote Function Calls .....	479
11.1.3	Challenges and Risks with Remote System Connections .....	480
11.1.4	Authorization Objects to Secure Your Remote Connections .....	481
11.1.5	Remote Function Call Callback Whitelisting .....	484
11.1.6	Remote Function Call Connections with Logon Data .....	486
<b>11.2</b>	<b>Best Practices .....</b>	<b>486</b>
11.2.1	Golden Rules .....	487
11.2.2	Interface User Best Practices .....	488
11.2.3	Interface Authorizations Best Practices .....	489
<b>11.3</b>	<b>SAP Unified Connectivity .....</b>	<b>491</b>
11.3.1	How Unified Connectivity Works .....	491
11.3.2	Unified Connectivity and Authorizations .....	492
<b>11.4</b>	<b>Xiting Authorizations Management Suite: Automated and Risk-Free Role Testing and Go-Live .....</b>	<b>493</b>
<b>11.5</b>	<b>Summary .....</b>	<b>494</b>

<b>12 Migrating Authorizations to SAP S/4HANA</b>	497
<b>12.1 Overview</b>	498
12.1.1 Simplifications within SAP S/4HANA	499
12.1.2 SAP S/4HANA Data Management Architecture	502
<b>12.2 SAP HANA Database</b>	504
12.2.1 User Types	505
12.2.2 SAP HANA Authorizations	506
<b>12.3 SAP S/4HANA Deployment Options</b>	507
12.3.1 SAP S/4HANA Cloud	508
12.3.2 SAP S/4HANA Cloud, Extended Edition	509
12.3.3 SAP S/4HANA Cloud, Private Edition	510
12.3.4 SAP S/4HANA: Managed by SAP HANA Enterprise Cloud	511
12.3.5 SAP S/4HANA: On-Premise or Managed by Hyperscale Cloud Providers	512
12.3.6 Comparison of SAP S/4HANA Deployment Options	513
<b>12.4 Business Process Changes through SAP S/4HANA</b>	516
<b>12.5 Core Data Services in SAP S/4HANA</b>	519
12.5.1 ABAP versus SAP HANA Core Data Services Views	520
12.5.2 Security in ABAP Core Data Services	521
12.5.3 ABAP Core Data Services View Troubleshooting	523
<b>12.6 Preparing for an SAP S/4HANA Migration</b>	527
12.6.1 Migration Considerations	527
12.6.2 SAP S/4HANA Approaches	528
12.6.3 Simplification Item Check	532
12.6.4 SAP Readiness Check	533
12.6.5 SAP Best Practices Explorer	534
12.6.6 SAP S/4HANA Migration Cockpit	535
12.6.7 Custom Code Validation	536
12.6.8 Regulatory Requirements and Compliance	539
<b>12.7 Migrating Authorizations to SAP S/4HANA with Standard SAP Tools</b>	541
12.7.1 Project Administration and Basis Activities	542
12.7.2 Analyzing Current Role Concepts	544
12.7.3 Upgrading and Maintaining Authorization Default Values	548
12.7.4 Analyzing SAP S/4HANA-Related Role Changes	550
12.7.5 Evaluating and Defining Job Function Roles	551
12.7.6 Transition and Enhancement of Roles for SAP S/4HANA	553
12.7.7 Testing Your Authorization Concept	556
12.7.8 Go-Live and Project Documentation	561

<b>12.8 Xiting Authorizations Management Suite: Helpful SAP S/4HANA Migration Features</b>	563
12.8.1 Comprehensive Usage Data Collection	563
12.8.2 Role Changes through the Simplification List	564
12.8.3 Security Concept	565
<b>12.9 Summary</b>	566
<b>13 Migrating Authorizations to SAP S/4HANA with the Xiting Authorizations Management Suite</b>	567
<b>13.1 SAP S/4HANA Migration Strategies with the Xiting Authorizations Management Suite</b>	568
13.1.1 Greenfield Migrations	569
13.1.2 Brownfield Migrations	572
<b>13.2 Preparation Phase: Role Concept Validation</b>	574
13.2.1 Verifying Role Concept Quality	575
13.2.2 Authorization Default Values Compliance	578
13.2.3 Consistency Verification of the Inheritance Concept	583
<b>13.3 Design Phase: Conceptual Role Migration</b>	583
13.3.1 Virtual Role Concept Design	584
13.3.2 Analyzing SAP S/4HANA-Related Role Changes	585
13.3.3 SAP Fiori Analysis	587
<b>13.4 Implementation Phase: SAP S/4HANA Role Implementation</b>	588
13.4.1 Role Migration to SAP S/4HANA	589
13.4.2 Extension of Roles with New SAP S/4HANA Functions	591
13.4.3 Template Roles Replication	595
<b>13.5 Validation Phase: SAP S/4HANA Role Concept Analysis</b>	599
13.5.1 Defining and Preparing Test Scenarios	600
13.5.2 Evaluating and Implementing of Test Results	601
<b>13.6 Activation Phase: Role Concept-Protected Go-Live</b>	605
13.6.1 End-User Cloning	605
13.6.2 Authorization Backups	607
<b>13.7 Summary</b>	609
The Authors	611
Index	613

# Index

## A

ABAP .....	29, 158
<i>authorizations</i> .....	51
<i>model</i> .....	29
ABAP Call Monitor .....	537
ABAP Debugger .....	343, 344
ABAP Development Tools .....	521, 538
ABAP List Viewer (ALV) .....	291, 408
<i>navigation</i> .....	214, 215
ABAP test cockpit .....	537, 538, 579
ABAP workbench .....	96
Access analysis service .....	443
Access certification service .....	445
Access governance	
<i>migration implications</i> .....	475, 476
Access management .....	24
<i>external requirements</i> .....	24
<i>internal requirements</i> .....	24
Access provisioning .....	42
Access request management (ARM)	
module .....	441
Access request service .....	444
Access risk analysis (ARA) module .....	440, 441
Access risks .....	450
ACID principle .....	112
Activated services .....	369
ACTVT field .....	139, 221, 222
<i>maintenance</i> .....	210
Add Missing Transaction Start	
Authorizations checkbox .....	227
Address tab .....	399
Amazon Web Service (AWS) .....	512
Analysis tools .....	316, 317
Analytic/structured privileges .....	38
Analyze transaction usage .....	547
Analyzing role concepts .....	544
API Finder .....	166, 168
App ID .....	358
App Launcher .....	359
App Support app .....	386, 387
Application navigation flags .....	219
Application privileges .....	38
Application start checks .....	75
Applications tab .....	251
Approval principle .....	51
auth/rfc_authority_check .....	482, 483
Authentication .....	23
AUTHORITY-CHECK statement .....	52, 75, 77, 86, 183, 185, 188, 240, 242, 282, 341, 342, 521
Authorization	
<i>backups</i> .....	607
<i>components</i> .....	52
<i>default values</i> .....	56
<i>download</i> .....	98
<i>object class</i> .....	52
Authorization checks .....	74, 149, 173
<i>deactivate</i> .....	85
<i>evaluate failures</i> .....	322, 323
<i>global deactivation</i> .....	85
<i>individual deactivation</i> .....	86
<i>required fields</i> .....	328
<i>SAP system</i> .....	80
<i>switchable</i> .....	81, 82, 84
Authorization concept .....	135
<i>analysis</i> .....	315
<i>bottom-up approach</i> .....	137, 139
<i>implementation</i> .....	136
<i>influences</i> .....	48
<i>principles</i> .....	49
<i>testing</i> .....	556
<i>top-down approach</i> .....	136–138
Authorization debugging .....	337, 339, 340
<i>navigation</i> .....	340
Authorization default values .....	184, 185
<i>advantages</i> .....	187
<i>check integrity</i> .....	241
<i>helpful tables</i> .....	190
<i>maintain</i> .....	548
<i>maintenance</i> .....	331, 560
<i>new statuses</i> .....	200
<i>optimization</i> .....	602, 603
<i>technical background</i> .....	188
<i>upgrading</i> .....	223
Authorization field .....	55, 103
AUTYP .....	61
<i>global deactivation</i> .....	212
<i>local deactivation</i> .....	213
<i>maintenance</i> .....	209
<i>program group maintenance</i> .....	211
<i>promote</i> .....	63, 64
<i>remove promoted field</i> .....	64
Authorization instances .....	294
Authorization level .....	103
Authorization maintenance .....	274
<i>best practices</i> .....	294, 295

- Authorization maintenance (Cont.)  
*buttons* ..... 275, 276
- Authorization object ..... 53, 206  
*TABU\_NAM* ..... 90  
*B\_MASSMAIN* ..... 211  
*F\_BKPF\_BUK* ..... 214  
*F\_KNAI\_GEN* ..... 328  
*F\_LFAI\_BUK* ..... 148, 150  
*K\_CCA* ..... 128  
*K\_KA\_RPT* ..... 211  
*K\_ORDER* ..... 128  
*K\_PCA* ..... 128  
*M\_EINK\_FRG* ..... 143  
*P\_ABAP* ..... 103, 128  
*P\_ORGIN* ..... 103, 105, 128  
*P\_ORGINCON* ..... 103, 105  
*P\_PCLX* ..... 103  
*P\_PERNR* ..... 103  
*P\_TCODE* ..... 103  
*PLOG* ..... 103  
*S\_ADMI* ..... 127  
*S\_ADMI\_FCD* ..... 207, 336  
*S\_ALV\_LAYO* ..... 206  
*S\_ALV\_LAYR* ..... 206  
*S\_ALV\** ..... 328  
*S\_ARCHIVE* ..... 127, 211  
*S\_BDC\_MONI* ..... 97  
*S\_BTCH\_ADM* ..... 97, 127  
*S\_BTCH\_JOB* ..... 97, 127  
*S\_BTCH\_NAI* ..... 97, 127  
*S\_BTCH\_NAM* ..... 127  
*S\_CTS\_ADMI* ..... 127  
*S\_CTS\_SADM* ..... 127  
*S\_DATASET* ..... 127  
*S\_DEVELOP* ..... 96, 127  
*S\_GUI* ..... 98, 206  
*S\_ICF* ..... 127, 481  
*S\_NUMBER* ..... 211  
*S\_PROG\** ..... 581  
*S\_PROGNAM* ..... 82, 83, 127, 211  
*S\_PROGRAM* ..... 92, 94, 127, 211, 580, 581  
*S\_PROJECT* ..... 328  
*S\_QUERY* ..... 95  
*S\_RFC* ..... 101, 127, 482, 487, 492, 493, 545, 573  
*S\_RFC\_ADM* ..... 127  
*S\_RFCACL* ..... 101, 102, 127, 481  
*S\_RZL\_ADM* ..... 127  
*S\_SCDO* ..... 127  
*S\_SECPOL* ..... 127  
*S\_SERVICE* ..... 544, 545, 558, 573  
*S\_SPO\_ACT* ..... 99, 127
- Authorization object (Cont.)  
*S\_SPO\_DEV* ..... 99, 127  
*S\_SPO\_PAGE* ..... 99  
*S\_START* ..... 545, 558, 573  
*S\_TABU\_CLI* ..... 90, 127, 207, 211  
*S\_TABU\_DIS* ..... 90, 95, 118, 127, 207, 211, 487  
*S\_TABU\_LIN* ..... 90, 127  
*S\_TABU\_NAM* ..... 90, 91, 95, 117, 118, 127, 207, 211, 217, 487  
*S\_TABU\_SQL* ..... 90, 127  
*S\_TABU\** ..... 580  
*S\_TCODE* ..... 75, 215, 217, 544, 545, 558, 573, 587, 590, 603  
*S\_TMS\_ACT* ..... 127  
*S\_TRANSLAT\** ..... 328  
*S\_TRANSPRT* ..... 127  
*S\_USER\_ADM* ..... 127  
*S\_USER\_AGR* ..... 127  
*S\_USER\_GRP* ..... 113, 127, 432, 451  
*S\_USER\_PRO* ..... 127  
*secure table access concept* ..... 90  
*statuses* ..... 277  
*update statuses* ..... 281, 282  
*validation* ..... 545
- Authorization profiles ..... 105  
*maintenance* ..... 593
- Authorization templates ..... 143, 144  
*button* ..... 193
- Authorization test evaluation ..... 559
- Authorization trace ..... 206, 329, 330  
*button* ..... 196
- Authorization values ..... 55
- Authorizations tab ..... 252
- Available transactions ..... 107
- B**
- Background jobs ..... 96, 97
- Basic authorization role ..... 140
- Basis ..... 239, 558
- Batch input sessions ..... 97
- Bluefield approach ..... 531
- Breakpoints ..... 338, 339, 343  
*create* ..... 341, 342
- Brownfield migration ..... 530, 531, 572  
*technical conversion indicators* ..... 573
- Business application programming  
 interfaces (BAPIs) ..... 488
- Business catalog ..... 370  
*create* ..... 371  
*new entities* ..... 372

- Business catalog (Cont.)  
*target mapping assignment* ..... 373, 374
- Business groups ..... 374  
*create* ..... 376
- Business partner approach ..... 518
- Business role management (BRM)  
 module ..... 441
- Business roles ..... 39, 359, 381
- Business transactions ..... 103
- C**
- C++ connector ..... 479
- CALL FUNCTION statement ..... 484
- Call stack analysis ..... 167
- CALL TRANSACTION statement ..... 216, 242
- Central user administration (CUA) ..... 255, 432  
*distribution paramers* ..... 433, 434  
*predelivered roles* ..... 433  
*tables* ..... 435
- Change documents ..... 164, 165
- Change role assignments ..... 412
- Change user documents ..... 406, 408
- Changed status ..... 279, 281
- Check modes ..... 181
- Check Values in Default Values checkbox ... 227
- Client configuration ..... 122
- Cloud connector ..... 42, 355
- Cloud solutions ..... 33
- Cockpit transactions ..... 220–222
- Code inspector ..... 537
- Code-based namespaces ..... 57  
*custom authorization objects* ..... 57
- Communication user ..... 397
- Complete missing modification flags  
 in SU24 data checkbox ..... 226
- Composite roles ..... 141, 145  
*maintenance* ..... 254  
*transport* ..... 307
- Compositie roles  
*creation* ..... 259, 260
- Conceptual approach ..... 381
- Conceptual role migration ..... 583, 585
- Consistency check ..... 238
- Continuous compliance ..... 457
- Control principle ..... 50
- Copy user ..... 406
- Core data services (CDS) ..... 519  
*ABAP security* ..... 521, 522  
*access policy* ..... 523  
*assignemnt roles* ..... 522  
*mapping roles* ..... 522
- Core data services (CDS) (Cont.)  
*troubleshooting* ..... 523, 524, 526  
*versus ABAP views* ..... 520
- Critical access scenarios ..... 88, 126, 128
- Critical action risks ..... 450
- Critical Authorization Framework (CRAF) .... 87
- Critical authorizations ..... 87, 126
- Critical permission risks ..... 450
- Cumulative processing logic ..... 55
- Custom authorizations  
*create* ..... 58  
*field* ..... 60, 61  
*object* ..... 58, 59
- Custom code validation ..... 536–538, 579, 581
- Custom transactions  
*create* ..... 112
- Customize security settings ..... 130
- Customizing roles ..... 265–268
- D**
- Data backup for Transaction SU24 ..... 230
- Data definition language (DDL) ..... 520
- Data model simplification ..... 499
- Database end users ..... 505
- Database management system  
 (DBMS) ..... 26, 405
- Debug and replace ..... 338
- Default communication assembly (CA) ..... 492
- Default data variants ..... 202, 203
- Default Values Comparison button ..... 193
- Defaults tab ..... 401
- Delete and recreate profile and  
 authorizations button ..... 276
- Delete Invalid Default Values checkbox .... 227
- Derived roles  
*creation* ..... 262, 263  
*maintain changes* ..... 264, 265
- Description tab ..... 249, 254
- Descriptor items ..... 363
- Dialog transactions ..... 108
- Dialog user ..... 396
- Disabled authorization check ..... 319
- Do Not Check status ..... 86
- Document analysis ..... 125
- Documentation tab ..... 398
- Download button ..... 193
- E**
- Edit old status button ..... 276
- Editions ..... 507



- Emergency access management (EAM) ..... 175, 176, 471  
*appropriate usage* ..... 472  
*module* ..... 442
- Employee group ..... 105
- Employee subgroup ..... 105
- Enabler role concept ..... 142
- Enabler roles ..... 145  
*authorize activity fields* ..... 150  
*determining use* ..... 147, 148, 150
- End-user cloning ..... 605–607
- Evaluating test results ..... 601
- Expert mode ..... 237
- ## F
- Finance and controlling integration ..... 518
- Firefighting ..... 471  
*functionalities* ..... 473, 474  
*provisioning strategies* ..... 474  
*types* ..... 473
- Four-eyes principle ..... 50
- Friends principle ..... 215
- Function code ..... 104
- Function testing ..... 556, 557
- Functional role ..... 140, 142
- Functions ..... 450
- ## G
- Go-live ..... 561, 562
- Good Manufacturing Practice (GMP) ..... 540
- Google Cloud ..... 512
- Greenfield migration ..... 529, 531, 569
- Groups tab ..... 404
- ## H
- Hewlett Packard Enterprise (HPE)  
 GreenLake ..... 512
- Hybrid system landscapes ..... 39  
*access risks* ..... 43
- Hyperscale cloud providers ..... 31, 512, 514
- ## I
- ID-based firefighter ..... 473
- Identity Authentication ..... 40, 42, 449
- Identity management principle ..... 49
- Identity Provisioning ..... 40, 449
- Inactive users ..... 415
- In-education help ..... 388, 389
- Infotype ..... 103
- Infrastructure as a service (IaaS) ..... 31
- Inheritance concept  
*verification* ..... 583
- Inheritance concept, verification ..... 583
- Initial role concept implementation  
*quick start* ..... 570  
*traditional* ..... 569
- Integrated trace ..... 206
- Integration testing ..... 558
- Interface authorizations, best practices ..... 489, 490
- Interface user, best practices ..... 488
- Internal Control System (ICS) ..... 594
- Internal security concept ..... 180
- Internet communication framework (ICF) ..... 101
- ## J
- Java connector ..... 479
- Java Database Connectivity (JDBC) ..... 504
- Job function ..... 551  
*evaluating roles* ..... 551, 552  
*principle* ..... 50  
*roles* ..... 380  
*trace* ..... 334, 335
- Job profile ..... 551
- Job-based role design ..... 138, 140
- ## K
- Kernel ..... 25  
*check* ..... 78  
*trace* ..... 490
- ## L
- Landscape simplification ..... 500
- Least privilege principle ..... 49
- Lenovo TruScale ..... 512
- Lic. Data tab ..... 405
- Lift and shift of authorizations ..... 572, 573
- Lock transactions ..... 120
- Locking status checks ..... 74
- Logon activity ..... 128
- Logon Data tab ..... 400, 401

- ## M
- Maintained status ..... 279
- Maintenance Area button ..... 197
- Manage check variants ..... 538
- Manage Launchpad Pages app ..... 365, 377
- Manage Launchpad Spaces app ..... 365, 377
- Manually status ..... 280, 281
- Mass user changes ..... 409, 411
- Master role ..... 261  
*creation* ..... 261
- Material ledger activation ..... 519
- Materials Management ..... 487, 501
- Menu bar and role information ..... 249
- Menu navigation ..... 216, 218  
*maintenance* ..... 217
- Menu tab ..... 255
- Merge Mode for PFCG button ..... 196
- Microsoft Azure ..... 512
- Migrate Your Data app ..... 535
- Migration considerations ..... 544, 545
- MiniApps tab ..... 253
- Mitigation ..... 457
- ## N
- Navigation considerations ..... 220
- Negative testing ..... 561
- NET connector for Microsoft ..... 479
- Normal users ..... 505
- ## O
- Object transactions ..... 109
- Object type ..... 104
- Object/SQL privileges ..... 38
- OData services ..... 359, 477  
*backend activation* ..... 367  
*description* ..... 366
- Open Data (OData) ..... 36
- Open Database Connectivity (ODBC) ..... 504
- OpenSQL ..... 521
- Organization value field ..... 139
- Organizational aspects ..... 542
- Organizational key ..... 105
- Organizational levels  
*create custom* ..... 61  
*maintenance* ..... 282, 283  
*maintenance best practices* ..... 284, 285
- Organizational rules ..... 454
- OrgSets ..... 171
- Other objects button ..... 196
- ## P
- Package privileges ..... 38
- Parameter checks ..... 77
- Parameter transactions ..... 110  
*create* ..... 116, 118
- Parameters tab ..... 403
- Password generation  
*blacklist* ..... 416  
*customizing switches* ..... 416  
*rules* ..... 415, 417
- Personalization tab ..... 253, 256, 404
- Personnel area ..... 105
- Plan version ..... 104
- Planning status ..... 104
- Plausibility checks ..... 76
- Positive testing ..... 559
- Post-process settings ..... 231
- Preparing test scenarios ..... 600, 601
- Principle of audit trails ..... 50
- Principle of critical authorizations ..... 49
- Privilege access management service ..... 446
- Privilege types ..... 506
- Process aspects ..... 543
- Process simplification ..... 499
- Productive system (PRD)  
*security analysis* ..... 121, 122
- Productive Test Simulation (PTS) ..... 290, 344, 490
- Profile generator ..... 65, 186, 189  
*header* ..... 247  
*initial screen* ..... 248  
*navigation* ..... 247  
*overview area* ..... 248
- Profile parameters  
*activation* ..... 319  
*rfc/callback\_security\_method* ..... 485
- Profiles ..... 67  
*manual* ..... 69  
*role* ..... 68  
*standard* ..... 69  
*tab* ..... 404
- Program access ..... 92, 93  
*tools* ..... 94
- Program code authority check ..... 78, 79
- Project views ..... 267
- Proposals ..... 183  
*data comparison* ..... 199, 200  
*data consistency check* ..... 230  
*maintenance* ..... 195–198  
*maintenance best practices* ..... 208  
*status* ..... 194

Proposals (Cont.)	
<i>system upgrade</i>	230
<i>upgrade process</i>	228, 229
<i>upgrade steps</i>	229
<i>upgrade tools</i>	224
Protected Go-Live (PGL)	605

## Q

Query access	94, 95
--------------	--------

## R

Read old status and merge with	
new data button	276
Reassess inconsistencies	232
Reference role	261
Reference user	173, 397
Regression testing	561
Relational database management system (RDBMS)	28
Release level/component version	358
Remediation	457
Remote function call (RFC)	100–102, 157, 477
<i>ABAP interfaces</i>	478
<i>authorization objects</i>	481, 482
<i>authorizations</i>	174
<i>callback destinations</i>	486
<i>callback security</i>	485
<i>callback whitelist</i>	484
<i>interfaces</i>	478
<i>non-SAP interfaces</i>	478
<i>trusted systems</i>	479
<i>uses</i>	478
<i>vulnerabilities</i>	481
Remote function modules (RFMs)	491–493
Remote system connections	480, 481
Remove Incorrectly-Defined SAP	
Organizational Level checkbox	227
Remove user roles	413
Repair bad field list in SU24 default	
values checkbox	225
Report	
<i>/SDF/RC_START_CHECK</i>	532
<i>Action Usage</i>	464
<i>AGR_RESET_ORG_LEVELS</i>	283
<i>Automatic comparison with Transaction SU22 data</i>	231
<i>Catalogs with content problems</i>	592
<i>Clean up application header data</i>	230
<i>Consistency check for default values</i>	230

Report (Cont.)	
<i>Critical auth watchdog and Critical combination watchdog</i>	594
<i>Migration of roles to S/4HANA</i>	586
<i>Modification Comparison with SU22 Data (2b)</i>	234, 235
<i>OData Services for SAP Fiori</i>	393
<i>PFCG_ORGFIELD_CREATE</i>	62
<i>PFCG_ORGFIELD_DELETE</i>	62
<i>PFCG_ORGFIELD_UPGRADE</i>	62, 233
<i>PRGN_COMPRESS_TIMES</i>	469
<i>Read old, merge new</i>	578, 593, 603
<i>Role Authorization Merger</i>	590
<i>RS_ABAP_SOURCE_SCAN</i>	80, 239, 240, 465
<i>RSAUDITC_BCE</i>	75
<i>RSCSAUTH</i>	94
<i>RSRFCCHK</i>	486
<i>RSUSR_AUTH_DATA_VERSION</i>	297
<i>RSUSR_DELETE_USERDOCU</i>	399
<i>RSUSR0003</i>	429
<i>RSUSR003</i>	129
<i>RSUSR008_009_NEW</i>	125
<i>RSUSRAUTH</i>	125
<i>SU24 cost.center rep. K_KA_RPT</i>	580
<i>SU24 from missing TSTCA</i>	580
<i>SU24 par.tcd. B_MASSMAIN</i>	580
<i>SU24 par.tcd. S_ARCHIVE</i>	580
<i>SU24 par.tcd. S_NUMBER</i>	580
<i>SU24 par.tcd. S_TABU* clusters</i>	580
<i>SU24 param.tcodes S_PROG*</i>	580
<i>SU24 param.tcodes S_TABU*</i>	580
<i>SU24 remove excessive values</i>	580
<i>SU24 report writer S_PROG*</i>	580
<i>SU24_AUTO_REPAIR</i>	225, 230, 232, 235
<i>SU24_Auto_Repair</i>	238
<i>SU24, Expert Mode for Transferring SU22 Data</i>	237, 238
<i>SUSR_TABLES_WITH_AUTH</i>	91
Report transactions	108
Restore backup transport	238
Restricted users	505
Ring buffer	321
RISE with SAP	516
Risk analysis	457
Risk mitigation	457
Risk recognition	456
Risk remediation	458
<i>approach</i>	460, 462
<i>business roles</i>	459
<i>composite roles</i>	459
<i>positions</i>	460

Risk remediation (Cont.)	
<i>single roles</i>	459
<i>users</i>	460
Risk Terminator	455
Role administration tables	257
Role building	257
<i>best practices</i>	292
Role concept analysis	599
Role concept reimplementation	571
Role concept validation	574
<i>verify quality</i>	575, 577
Role creation	256
Role derivation	141
Role design	
<i>approaches</i>	135
<i>trends</i>	136
Role design concepts	
<i>comparison</i>	145, 146
Role design service	444, 448
Role implementation	588
Role maintenance	
<i>best practices</i>	291
Role menu	250
Role menu comparison	273
Role menu objects	270
<i>maintenance</i>	270, 271
Role migration	589, 591
Role naming convention	152–154, 258, 381
Role profiles	
<i>generate</i>	296
<i>mass generation</i>	304, 305
<i>up-to-dateness</i>	582
Role quality	125
Role templates	268
Role transport	306–308
Role versioning	297–299
Role-based firefighter	473
Role-mining strategies	43
Roles	65
<i>advantages</i>	246
<i>analysis</i>	125
<i>assign and remove</i>	269
<i>authorization</i>	66
<i>button</i>	197
<i>composite</i>	67
<i>delta analysis</i>	603, 605
<i>mass maintenance</i>	301–303
<i>mass user comparison</i>	305
<i>menu</i>	66
<i>overview status</i>	299
<i>single</i>	66, 67
<i>tab</i>	255, 403

Roles (Cont.)	
<i>tracing</i>	287–289
<i>users</i>	66
Rule building and validation	456
Ruleset	
<i>architecture</i>	451
<i>change</i>	452
<i>components</i>	449, 450
<i>custom transactions</i>	463–466
<i>standard</i>	452, 453

## S

S_A.DEVELOP profile	70
S_A.SYSTEM profile	70
S4HANA_READINESS_1909 check	
variant	538
S4HANA_READINESS_2020 check	
variant	538
S4HANA_READINESS_REMOTE check	
variant	538
Sales Performance – Plan/Actual – for Sales Manager app	369
SAP Access Control	41, 42, 44, 137, 152, 439, 440, 442, 448, 449, 458, 462, 467, 472, 475, 541
<i>benefits</i>	440
<i>business roles</i>	468–470
SAP Analysis for Microsoft Office	504
SAP Analytics Cloud	504
SAP Application Interface Framework	286
SAP Ariba	33, 443
SAP Best Practices Explorer	382, 517, 528, 534, 535, 552
SAP Business Client	34, 396
SAP Business Suite	27, 30, 94, 106, 514
SAP Business Technology Platform (SAP BTP)	39, 354, 448, 508, 514
SAP Business Warehouse (SAP BW)	102, 142, 177, 286, 287
SAP BusinessObjects Business Intelligence	504
SAP Cloud	39
SAP Cloud Identity Access	
Governance	41–44, 439, 443, 444, 448, 449, 454, 473, 475
<i>bridge</i>	447, 448
<i>core functionality</i>	443
<i>key capabilities</i>	447
SAP Cloud Identity Services	40
SAP Code Vulnerability Analyzer	538
SAP Customer Relationship Management (SAP CRM)	102

SAP Data button ..... 196  
 SAP Data Services ..... 528  
 SAP Enterprise Portal ..... 26  
 SAP ERP ..... 26, 497, 501  
 SAP ERP Human Capital Management  
   (SAP ERP HCM) ..... 89, 212, 253, 256, 439, 558  
   *all access* ..... 105, 106  
   *authorizations* ..... 102  
 SAP Fieldglass ..... 33  
 SAP Fiori ..... 29  
   *apps reference library* ..... 356–358  
   *architecture* ..... 351, 352  
   *check authorization concept* ..... 591  
   *concept implementation* ..... 369  
   *general end-user role* ..... 383, 384  
   *legacy apps* ..... 351  
   *principles* ..... 349, 350  
   *reporting and troubleshooting*  
     *transactions* ..... 390, 391  
   *role analysis* ..... 588  
   *role building* ..... 385  
   *role checklist* ..... 384, 385  
   *role concept* ..... 380  
   *role preparation* ..... 382, 383  
   *search* ..... 351  
   *troubleshooting* ..... 386  
   *UI* ..... 36  
 SAP Fiori Apps Recommendations  
   Report ..... 550  
 SAP Fiori launchpad ..... 351, 352, 384, 554  
   *app manager* ..... 363  
   *central hub deployment* ..... 354  
   *content manager* ..... 362, 371, 385  
   *deployment options* ..... 353  
   *designer* ..... 360, 361, 385  
   *embedded deployment* ..... 353  
   *intent-based navigation* ..... 372  
   *personalization* ..... 378  
   *role menu objects* ..... 555  
 SAP GUI ..... 34  
 SAP HANA ..... 28, 29, 520  
   *authorizations* ..... 506  
   *database* ..... 504  
   *native authorizations* ..... 37  
   *privilege framework* ..... 37  
   *privileges* ..... 506  
   *roles* ..... 507  
   *security mechanisms* ..... 37  
   *user types* ..... 505  
 SAP HANA Enterprise Cloud ..... 507, 511  
 SAP Identity Management  
   (SAP ID Management) ..... 41, 42, 151, 543  
 SAP Integrated Business Planning  
   for Supply Chain (SAP IBP) ..... 33  
 SAP Launchpad service ..... 355  
   *benefits* ..... 355, 356  
 SAP Lumira ..... 504  
 SAP NetWeaver ..... 26, 28, 212  
 SAP ONE Support Launchpad ..... 532  
 SAP R/3 ..... 26  
 SAP Readiness Check ..... 528, 533, 534  
 SAP Readiness Check for SAP S/4HANA ..... 502  
 SAP S/4HANA ..... 27, 28, 498, 511, 512, 514  
   *analyze role changes* ..... 550  
   *business process changes* ..... 516, 517  
   *data management architecture* ..... 502  
   *deployment* ..... 30–32  
   *deployment options* ..... 507, 513  
   *migration approaches* ..... 528, 531, 542,  
     553, 554  
   *preparing for migration* ..... 527, 528  
   *regulatory requirements* ..... 539, 540  
   *role concept* ..... 570  
   *simplification list* ..... 501, 502  
   *simplifications* ..... 499  
   *standard migration tools* ..... 541  
 SAP S/4HANA Cloud ..... 32, 33, 500, 508,  
   509, 514  
 SAP S/4HANA Cloud, extended  
   edition (EX) ..... 509, 510, 514  
 SAP S/4HANA Cloud, private  
   edition ..... 510, 511, 514  
 SAP S/4HANA Finance ..... 518  
 SAP S/4HANA migration cockpit ..... 528, 535, 536  
 SAP Solution Manager ..... 180, 280, 286, 287  
 SAP standard profiles ..... 128  
 SAP standard users ..... 129  
 SAP SuccessFactors ..... 33, 439, 443  
 SAP Supplier Lifecycle Management ..... 501  
 SAP Supplier Relationship Management  
   (SAP SRM) ..... 102, 501  
 SAP Support Portal ..... 239  
 SAP Transformation Navigator ..... 516  
 SAP Transport Management System  
   (STMS) ..... 178  
 SAP UI technology support ..... 386  
 SAP Web Dispatcher ..... 351  
 SAP\_ALL profile ..... 70, 105, 106  
 SAP\_NEW profile ..... 70  
 SAPUI5 ..... 29, 36  
   *applications* ..... 351, 359  
 Search for Obsolete Applications (2d) ..... 236  
 Securing interfaces ..... 487  
 Security audit log configuration ..... 122

Security compliance assurance ..... 594  
 Security control matrix ..... 50  
 Segregation of duties (SoD) ..... 50, 137, 138, 146  
   *best practices* ..... 147  
   *continuous monitoring* ..... 462, 463  
   *management* ..... 456  
   *phases* ..... 456  
   *risks* ..... 450  
   *role calculation* ..... 146  
   *SoD principle* ..... 51  
 Selection screen options ..... 193  
 Separate proposal data ..... 118, 119  
 Service user ..... 397  
 Simplification item check ..... 532, 533  
 Simplification list ..... 585  
   *role changes* ..... 564  
 Single roles ..... 139–141, 145  
   *creation* ..... 259  
   *maintenance area* ..... 248  
   *transport* ..... 307  
 SNC tab ..... 401  
 Software as a service (SaaS) ..... 31  
 Spaces and pages ..... 377  
   *create* ..... 377  
   *OData services* ..... 377  
 Spool authorizations ..... 98, 99  
 Standard principle ..... 51  
 Standard status ..... 278  
 Standard users ..... 428  
   *disable automatic creation* ..... 428  
   *security* ..... 428  
 Standard-compliant role concept  
   *migration* ..... 573  
 Standards compliance ..... 578  
 Start authorization objects ..... 75  
 Subtype ..... 105  
 Sustainable role building ..... 290  
 System changeability ..... 122  
 System configuration analysis ..... 122  
 System layer  
   *alignment* ..... 191  
   *proposal maintenance* ..... 191  
 System privileges ..... 38  
 System user ..... 396  
**T**  
 Table  
   ACDOCA ..... 519  
   ADR2 ..... 422  
   ADR3 ..... 422  
   ADR6 ..... 422  
 Table (Cont.)  
   ADRP ..... 422  
   AFRU ..... 117, 118  
   AGR\_1016 ..... 258  
   AGR\_1251 ..... 125, 258, 545  
   AGR\_1252 ..... 64, 258  
   AGR\_AGRS ..... 258  
   AGR\_BUFFI ..... 258  
   AGR\_DEFINE ..... 258  
   AGR\_PROF ..... 258  
   AGR\_TCODES ..... 545  
   AGR\_TEXTS ..... 258  
   AGR\_TIME ..... 258  
   AGR\_USERS ..... 258  
   BUTOOO ..... 92  
   DDO2L ..... 191  
   GRACACTUSAGE ..... 437  
   PRGN\_CUST ..... 131, 132, 308, 415  
   SSM\_CUST ..... 132  
   SU2X\_TEXT ..... 202  
   TOOO ..... 110  
   TADIR ..... 191  
   TCURR ..... 91, 92  
   TDDAT ..... 91, 190, 205  
   TOBJ ..... 61  
   TPGP ..... 94  
   TRDIR ..... 94, 191  
   TSTC ..... 74, 80, 191  
   TSTCA ..... 76, 80, 191, 213  
   TSTCP ..... 118, 191, 212  
   TSTCT ..... 191, 210, 464  
   USER\_ADDR ..... 422  
   USERSYSUPL ..... 435  
   USERSYSUPL ..... 435  
   USHO2 ..... 422  
   USHO4 ..... 422  
   USLAO4 ..... 435  
   USOBAUTHINACTIVE ..... 76  
   USOBT ..... 57, 79, 188, 190, 199, 227, 231  
   USOBT\_C ..... 57, 190, 199, 223, 227, 230, 236  
   USOBX ..... 57, 188, 190, 199, 227  
   USOBX\_C ..... 57, 199, 223, 227, 230, 236  
   USORG ..... 212  
   USR\_CUST ..... 133, 422  
   USRO1 ..... 421  
   USRO2 ..... 88, 396, 421  
   USRO3 ..... 421  
   USRO4 ..... 422  
   USRO5 ..... 422  
   USRO9 ..... 422  
   USR10 ..... 422  
   USR11 ..... 422

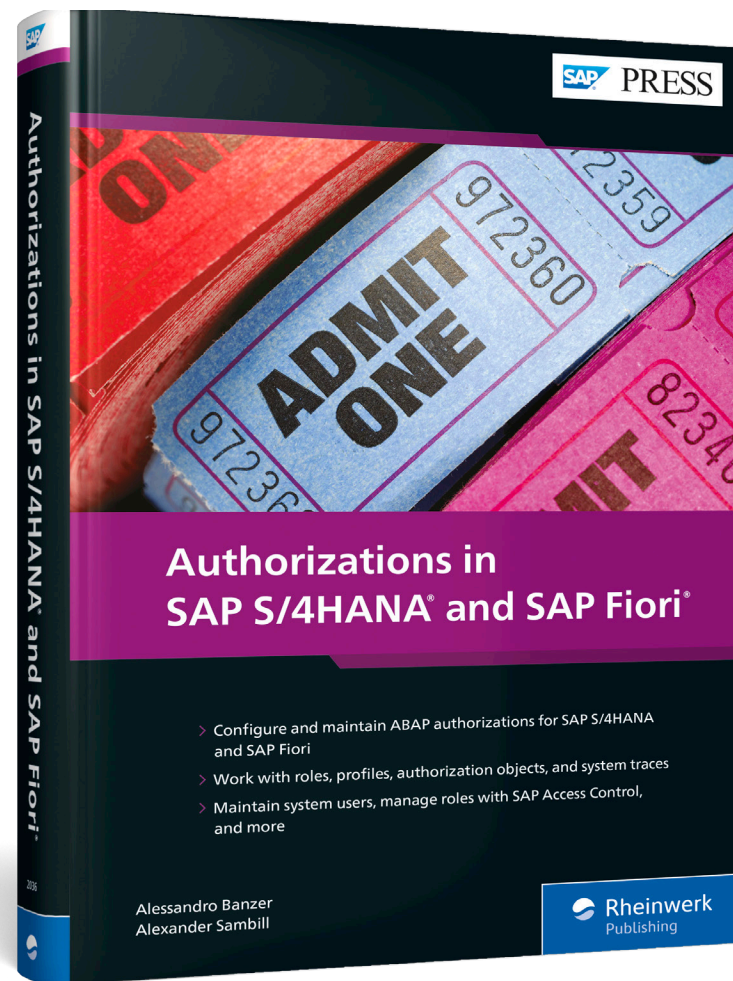
Table (Cont.)	Transaction (Cont.)
<i>USR12</i> ..... 422	/ <i>UI2/FLP_SYS_CONF</i> ..... 379
<i>USR21</i> ..... 422	/ <i>UI2/FLPAM</i> ..... 363
<i>USR40</i> ..... 416, 422	/ <i>UI2/FLPCM_CONF</i> ..... 362
<i>USRPWDHISTORY</i> ..... 422	/ <i>UI2/FLPCM_CUST</i> ..... 362, 371
<i>USRSYSACT</i> ..... 435	/ <i>UI2/FLPD_CONF</i> ..... 360
<i>USRSYSACTT</i> ..... 435	/ <i>UI2/FLPD_CUST</i> ..... 360, 376
<i>USRSYSLNG</i> ..... 435	/ <i>UI2/FSAC</i> ..... 391
<i>USRSYSPRF</i> ..... 435	/ <i>XITING/TIMES_MULTI</i> ..... 607
<i>USRSYSPRFT</i> ..... 435	<i>AUTH_SWITCH_OBJECTS</i> ..... 85
<i>V_BRG_54</i> ..... 91	<i>BP</i> ..... 118, 203, 220, 295, 518, 585
Table access ..... 89	<i>F9SH</i> ..... 234
<i>security risks</i> ..... 89	<i>FBO1</i> ..... 26, 328
<i>standard tools</i> ..... 90	<i>FBO3</i> ..... 184–186, 189, 214, 278, 323
<i>transparent</i> ..... 91	<i>FB60</i> ..... 455
Table auditing ..... 124	<i>FD15</i> ..... 209
Table security ..... 124	<i>FDKUSER</i> ..... 328
Target mapping ..... 359	<i>FKO1/O2</i> ..... 461
Task-based roles ..... 139	<i>FKO2</i> ..... 335, 455
Technical analysis ..... 166	<i>FKO3</i> ..... 148, 149, 335
Technical aspects ..... 543	<i>FSOO</i> ..... 518
Technical catalog ..... 370	<i>IWFND/ERROR_LOG</i> ..... 390
Technical configuration ..... 359	<i>KA01</i> ..... 518
Technical users ..... 505	<i>KA02</i> ..... 518
Template roles	<i>KA03</i> ..... 518
<i>replication</i> ..... 597	<i>LAST_SHORTDUMP</i> ..... 554
Template roles, replication ..... 595, 597	<i>LSMW</i> ..... 536
Test plan ..... 559	<i>LPMC</i> ..... 535
Three-tier deployment ..... 502	<i>ME2IN</i> ..... 126, 450, 468
Time Entry app ..... 379	<i>ME22N</i> ..... 450, 468
Traces ..... 315, 324, 326	<i>ME23N</i> ..... 468
<i>authorization error</i> ..... 326–328	<i>ME24(N)</i> ..... 143
<i>populating data</i> ..... 205–207	<i>ME29N</i> ..... 126
<i>use cases</i> ..... 320	<i>MIGO</i> ..... 220, 222, 295
Tracing applications ..... 331	<i>MMO3</i> ..... 209
Traffic light icons ..... 277	<i>PA10</i> ..... 103
Transaction	<i>PA20</i> ..... 103
/ <i>IWBEP/CACHE_CLEANUP</i> ..... 391	<i>PA30</i> ..... 103
/ <i>IWBEP/ERROR_LOG</i> ..... 391	<i>PA40</i> ..... 103
/ <i>IWBEP/VIEW_LOG</i> ..... 391	<i>PA51</i> ..... 103
/ <i>IWFND/APPS_LOG</i> ..... 390	<i>PFCG</i> ..... 62, 65–69, 75–77, 80, 102, 108, 145,
/ <i>IWFND/CACHE_CLEANUP</i> ..... 390	150, 160, 170, 172, 178, 189, 196, 220, 230,
/ <i>IWFND/MAINT_SERVICE</i> ..... 367, 368, 390	235, 246, 247, 254, 260–262, 267, 269, 273,
/ <i>N/XITING/ROLEDESIGNER</i> ..... 160	280, 287, 288, 291, 297, 299, 304, 307, 308,
/ <i>UI2/CHIP_SYNCHRONIZE_CACHE</i> ..... 390	326, 335, 349, 377, 385, 455, 482, 487, 489,
/ <i>UI2/DELETE_CACHE</i> ..... 391	494, 506, 508, 509, 513, 522, 552, 563, 589
/ <i>UI2/FLC</i> ..... 391	<i>PFCGMASSVAL</i> ..... 301–304
/ <i>UI2/FLC1</i> ..... 391	<i>PFUD</i> ..... 256, 269
/ <i>UI2/FLIA</i> ..... 391	<i>PMO1</i> ..... 103
/ <i>UI2/FLP</i> ..... 384	<i>PRGN_COMPARE_ROLE_MENU</i> ..... 391
/ <i>UI2/FLP_CUS_CONF</i> ..... 379	<i>RSAU_CONFIG</i> ..... 122
/ <i>UI2/FLP_DEL_PERS</i> ..... 379	<i>RSPFPAR</i> ..... 124

Transaction (Cont.)	Transaction (Cont.)
<i>RSRTS_ODP_DIS</i> ..... 524	<i>SM30</i> ..... 76, 88, 90–92, 110, 116, 126, 130,
<i>RSRTS_QUERY_CHECK</i> ..... 524	162, 205, 415, 432, 435, 465
<i>RSUSR_ROLE_MENU</i> ..... 391	<i>SM31</i> ..... 90
<i>RSUSR_START_APPL</i> ..... 391	<i>SM34</i> ..... 90, 126, 162
<i>RSUSR200</i> ..... 128	<i>SM35</i> ..... 97
<i>RZ10</i> ..... 85, 86, 99, 195, 320	<i>SM36</i> ..... 97
<i>S_ALR_87101219</i> ..... 91	<i>SM37</i> ..... 97
<i>S416H</i> ..... 89	<i>SM59</i> ..... 101, 479, 481, 484, 486
<i>S416N</i> ..... 88, 89	<i>SMX</i> ..... 97, 554
<i>S4H16H</i> ..... 88	<i>SPOO</i> ..... 99
<i>S4H16N</i> ..... 88	<i>SPO1</i> ..... 99
<i>SA38</i> ..... 75, 80, 88, 92, 93, 111, 125, 126, 129,	<i>SPO2</i> ..... 99, 554
162, 239, 283, 335, 465	<i>SPI2</i> ..... 99
<i>SACF</i> ..... 76, 81–84	<i>SPAD</i> ..... 99
<i>SACF_COMPARE</i> ..... 82, 84	<i>SPRO</i> ..... 265, 267, 455
<i>SACF_INFO</i> ..... 84	<i>SPRO_ADMIN</i> ..... 265, 267
<i>SACF_TRANSFER</i> ..... 84	<i>SQ00</i> ..... 94, 95
<i>SACM</i> ..... 391, 524, 526	<i>SQ01</i> ..... 94, 95
<i>SCC4</i> ..... 110, 122, 216, 455	<i>SQ02</i> ..... 95
<i>SCC5</i> ..... 120	<i>SQ03</i> ..... 95
<i>SCI</i> ..... 537, 539	<i>SQVI</i> ..... 94
<i>SCMON</i> ..... 537	<i>SSM2</i> ..... 401
<i>SCOT</i> ..... 109	<i>STO1</i> ..... 317, 318, 320, 323–325
<i>SCTS_RSWBO004</i> ..... 122	<i>STO1/STAUTHTRACE</i> ..... 316
<i>SCUM</i> ..... 433	<i>STO1/STAUTHTRACE</i> ..... 488
<i>SDDLAR</i> ..... 524	<i>STO3(N)</i> ..... 489
<i>SEO6</i> ..... 216, 218	<i>STO3N</i> ..... 177, 234, 238, 358, 393, 436, 464,
<i>SEO9</i> ..... 307	547, 551, 552, 563
<i>SE16</i> ..... 88, 89, 92, 95, 110, 116, 118, 124, 126,	<i>STO5</i> ..... 524
162, 205, 331, 435, 465, 486, 545	<i>STAD</i> ..... 325
<i>SE16(N)</i> ..... 202, 369, 391, 546	<i>START_REPORT</i> ..... 92, 111
<i>SE16H</i> ..... 89	<i>STAUTHTRACE</i> ..... 323
<i>SE16N</i> ..... 89, 162, 465, 486	<i>STAUTHTRACE</i> ..... 239, 288, 317, 320, 324,
<i>SE17</i> ..... 90	325, 346, 523, 524, 558, 560
<i>SE37</i> ..... 126	<i>STAUTHTRACE/STO1</i> ..... 391, 489
<i>SE38</i> ..... 111, 126, 162, 464, 465, 532, 538	<i>STCO1</i> ..... 368
<i>SE54</i> ..... 91	<i>STDDAT</i> ..... 91
<i>SE80</i> ..... 464, 524, 538	<i>STMS</i> ..... 124, 216–218, 307
<i>SE84</i> ..... 379	<i>STMS_EXPORT</i> ..... 218
<i>SE93</i> ..... 77, 115, 117, 118, 197, 213, 464	<i>STMS_IMPORT</i> ..... 218
<i>SE97</i> ..... 219	<i>STRFCTRACE</i> ..... 318
<i>SECPOL</i> ..... 423, 424	<i>STSIMAUTHCHECK</i> ..... 316, 317, 335, 558,
<i>SHDO</i> ..... 112	560, 562
<i>SIFC</i> ..... 369	<i>STSIMAUTHTRACE</i> ..... 335
<i>SLG1</i> ..... 391	<i>STUSERTRACE</i> ..... 239, 316, 317, 320, 333,
<i>SMO1</i> ..... 120	489, 558, 560
<i>SMO1_CUS</i> ..... 120	<i>STUSOBTRACE</i> ..... 205, 209, 239, 316, 317,
<i>SMO1_DEV</i> ..... 120	320, 329–331, 333, 490, 558
	<i>SU_VCUSRVARCOM_CHAN</i> ..... 125

- Transaction (Cont.)
- SU01* ..... 73, 74, 108, 110, 112, 113, 115, 162, 195, 197, 220, 254, 260, 269, 339, 341, 397, 398, 400, 403, 405, 406, 415, 427, 430, 431, 451, 473, 505, 508, 509, 513
  - SU01D* ..... 162, 222
  - SU02* ..... 65, 69
  - SU10* ..... 269, 404, 409, 411, 415, 427
  - SU21* ..... 54, 58, 60, 69, 225
  - SU22* ..... 57, 62, 100, 124, 188, 189, 223, 226, 227, 230, 238, 548, 549, 578
  - SU24* ..... 57, 59, 62, 86, 91, 92, 95, 108, 110–112, 115, 116, 118–120, 144, 150, 151, 167, 177, 178, 184–186, 189, 192, 194–200, 202, 203, 206, 208, 209, 211, 212, 215, 218, 220, 222, 224, 225, 227, 230, 231, 234, 238, 239, 241, 242, 251, 277, 278, 280, 281, 286, 287, 292, 294, 295, 305, 326, 331–333, 383, 465, 467, 468, 488–490, 494, 548, 555, 575, 578–580, 590, 602
  - SU25* ..... 85, 100, 124, 188, 191, 193, 196, 212, 224, 226, 228–231, 235, 236, 295, 383, 391, 548–550, 557, 575, 578, 586
  - SU3* ..... 401, 403, 554
  - SU53* ..... 239, 289, 316, 318, 320, 321, 342, 344, 386, 524, 560, 562
  - SU54* ..... 554
  - SU55* ..... 558
  - SU56* ..... 72, 149, 321, 417
  - SUCOMP* ..... 400
  - SUI\_SUPPORT* ..... 386
  - SUIM* . 87, 91, 94, 125, 128, 220, 404, 421, 546
  - SUPC* ..... 296, 304
  - SUPO* ..... 61–64
  - TCODE* ..... 167
  - XK01/02* ..... 461
  - ZDELETEUSER* ..... 468
  - ZSEI6\_AFRU* ..... 118
  - ZSEI6\_TDDAT* ..... 208
  - ZSU01\_VAR\_LOCK* ..... 110, 115
- Transaction types ..... 106
- Troubleshooting system upgrade ..... 238
- TSTC check ..... 74
- TSTCA check ..... 76
- Two-tier deployment ..... 502, 503
- U**
- Unified Connectivity ..... 318, 491–493
- Universal journal ..... 519
- Upgrading customer-specific organizational levels ..... 233
- Upload button ..... 193
- User acceptance test (UAT) ..... 560
- User access ..... 25
- User access review (UAR) ..... 422, 470, 471
- User analysis ..... 128
- User buffer ..... 25, 417, 418
- User classification ..... 421
- User creation, navigation ..... 397
- User experience (UX) ..... 23, 35
- User groups
- assign* ..... 432
  - maintain* ..... 430, 431
- User IDs ..... 420
- User interface (UI)
- simplification* ..... 500
- User maintenance tabs ..... 398
- User master record ..... 395
- lock status* ..... 423
  - maintenance* ..... 396
  - security policies* ..... 423–426
- User tab ..... 253, 256
- User-related tables ..... 421, 422
- Users ..... 70
- buffer* ..... 72
  - maintenance* ..... 73
  - master record* ..... 71
  - naming conventions* ..... 419, 420
  - trace* ..... 335–337
  - types* ..... 73, 396, 397
- V**
- Vacation Request app ..... 379
- Value help ..... 100
- Variant transactions ..... 109
- create* ..... 112, 113, 115
- Virtual data models (VDMs) ..... 503
- W**
- Web Dynpro ..... 25
- Where-used list ..... 285, 286
- Workflow tab ..... 251
- Workload Monitor ..... 436, 437
- Written form principle ..... 51
- X**
- Xiting ABAP Alchemist ..... 158, 165, 166, 242, 466, 467
- features* ..... 166

- Xiting Authorizations Management Suite (XAMS) ..... 87, 157–159, 490, 567
- authorize remote call function interfaces* ..... 494
  - migration tools* ..... 563
  - SAP S/4HANA migration* ..... 568
- Xiting Automatic Role Builder ..... 603
- Xiting Productive Test Simulation (PTS) ..... 570
- Xiting Quick Start (XQS) ..... 569, 570
- Xiting RFC Stocktake Tool ..... 159
- Xiting Role Builder ..... 159, 172, 174, 344, 345, 608
- Xiting Role Builder Coverage Analyzer ..... 346, 603, 604
- Xiting Role Designer ..... 158–160, 308, 563, 584, 585, 587, 589
- business data reporting* ..... 164
  - design cockpit* ..... 310
- Xiting Role Designer (Cont.)
- function module reporting* ..... 163
  - project cockpit* ..... 309
  - project reporting* ..... 311
  - reporting* ..... 162
  - transaction reporting* ..... 163
  - virtual design cockpit* ..... 161
- Xiting Role Profiler ..... 159, 176, 241, 393, 575, 577, 580, 583, 589
- reporting* ..... 177, 178
- Xiting Role Replicator ..... 159, 169, 171, 172, 311, 392, 594, 596–599, 601, 607
- bulk processing* ..... 170
  - OrgSets* ..... 170
- Xiting Security Architect ..... 159, 179, 180, 182, 565
- concept templates* ..... 180
- Xiting Times ..... 159, 172, 175, 176, 600, 605, 606, 608
- Xiting User Locking Tool ..... 159





Alessandro Banzer, Alexander Sambill

## Authorizations in SAP S/4HANA and SAP Fiori

625 pages, 2022, \$89.95

ISBN 978-1-4932-2036-6

 [www.sap-press.com/5203](http://www.sap-press.com/5203)



**Alessandro Banzer** is the chief executive officer of Xiting. He has worked in information technology since 2004, specializing in SAP since 2009. Since then, Alessandro has been involved with global SAP projects in various roles. Alessandro is an active contributor and moderator in the governance, risk, and compliance space on

SAP Community, as well as a speaker at SAPHIRE, ASUG, SAPinsider, and other SAP-related events. He holds a degree in business information technology, as well as an Executive Master of Business Administration from Hult International Business School in London, UK.



**Alexander Sambill** is a senior SAP security consultant and certified SAP trainer at Xiting Germany. He is a security-minded professional with consulting and sales experience in many industries. During his years of work within SAP security, he specialized himself for SAP authorizations in SAP ERP and SAP S/4HANA with

SAP Fiori. Alexander leads authorization migration and redesign projects for small and large enterprises, educates customers, and solves individual custom use cases. He is also a federally certified instructor (IHK) in commerce and industry. Alexander is a passionate writer and active blogger of technical and scientific articles, e-books, white papers, surveys, and more about SAP security and authorizations. He is also the content manager of publications for SAP authorizations at Xiting AG.

*We hope you have enjoyed this reading sample. You may recommend or pass it on to others, but only in its entirety, including all pages. This reading sample and all its parts are protected by copyright law. All usage and exploitation rights are reserved by the author and the publisher.*