Manage Business Roles in SAP Cloud Identity Access Governance (IAG) to Ease the Maintenance of SAP Cloud and On-Premise Access across Systems

Dina Shahin, Principal Advisor Europe, Customer Advisory Group LLC

SAPinsider
Las Vegas

2023

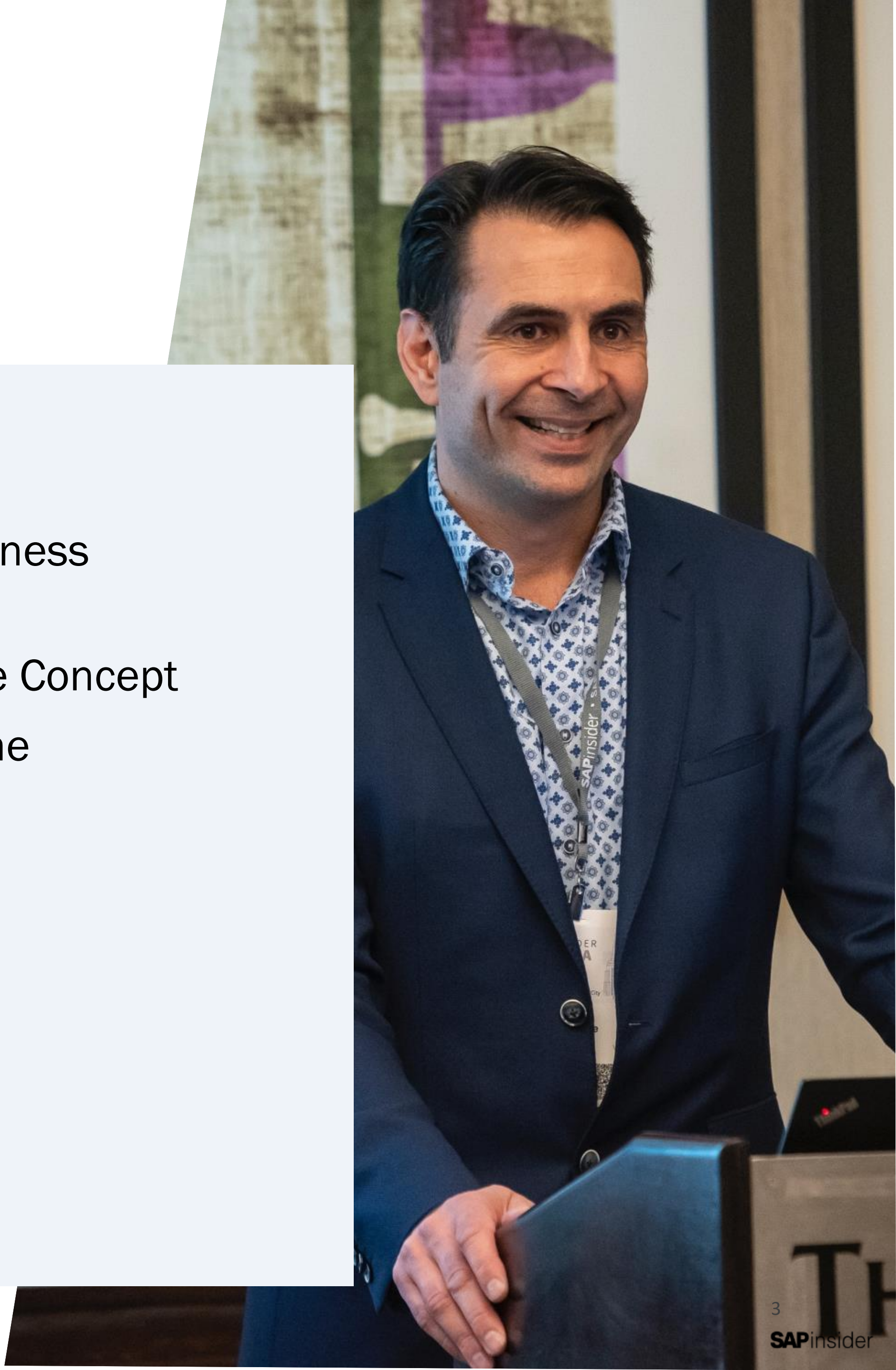
SAPinsider

In This Session

Attend this session to see a detailed examination of the "Role Designer" Business Role Management in SAP Cloud Identity Access Governance (IAG). We will take a deep dive into how to set up and maintain Business Roles. This session will cover for which applications Business Roles are required, as well as for which applications setting up Business Roles makes sense. Best Practice when setting up Business Roles manually as well when utilizing the Role Mining capabilities will be covered.

What We’ll Cover

- What is a Business Role?
- Functionality and Technical Setup around Business Roles
- Steps and Effort to Implement a Business Role Concept
- Examine the pros and cons of implementing the Business Role
- Wrap-Up



What Is a Business Role?

Technically, a Business Role is a composite role of access across multiple systems connected with IAG. Business roles reside solely in IAG and have no equivalent in any connected system.

Within Privileged Access Management only Business Roles can be assigned to Privileged Users (FireFighters). Even if that requires the set up of one-to-one relationships (one Business Role contains only one role / access from the back-end systems), those Business Roles need to be set up. Access from systems connected to IAG cannot be granted directly to PAM Users.

What Is a Business Role?

Nowadays when users request access, they have to request multiple access with one single system as well as across several systems.

For example, as an Accounts Payables Manager, you will need access in ECC/S/4 systems, BI systems for reporting, and HR/SuccessFactors to manage your team members.

In order to ease requesting access, the access required can be grouped in Business Roles. Instead of requesting access step by step when finding out, you are missing some access, users can request the complete set of access they require to fulfill their role or position within the company.

What Is a Business Role?

Business Roles can be set up to cover:

- Position-based access
- Role-based access

The definition how you want to use Business Roles depends entirely on your requirements within your organization.

Also, role/access bundles that should be granted to all users (e.g., timesheet entry) can be gathered in Business Roles.

Functionality Around Business Roles

Business Roles can be used/analyzed with the following modules in IAG:

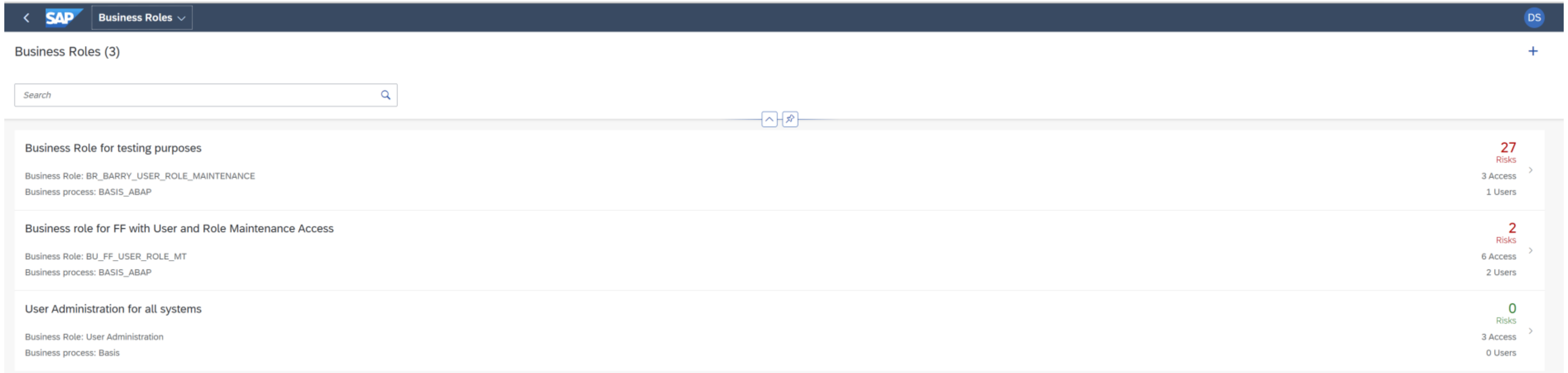
- Access Analysis
- Privilege Access Management
- Access Request

Functionality Around Business Roles – Access Analysis

Access Analysis is not only carried out on the access/roles from the backend system, but also on Business Role Level.

So, an analysis can be carried out not only on single roles but on a combination of roles/access given to end-users.

This prevents surprises when requesting/assigning a bundle of access to users.



Business Roles (3)

Business Role for testing purposes
Business Role: BR_BARRY_USER_ROLE_MAINTENANCE
Business process: BASIS_ABAP
27 Risks
3 Access
1 Users

Business role for FF with User and Role Maintenance Access
Business Role: BU_FF_USER_ROLE_MT
Business process: BASIS_ABAP
2 Risks
6 Access
2 Users

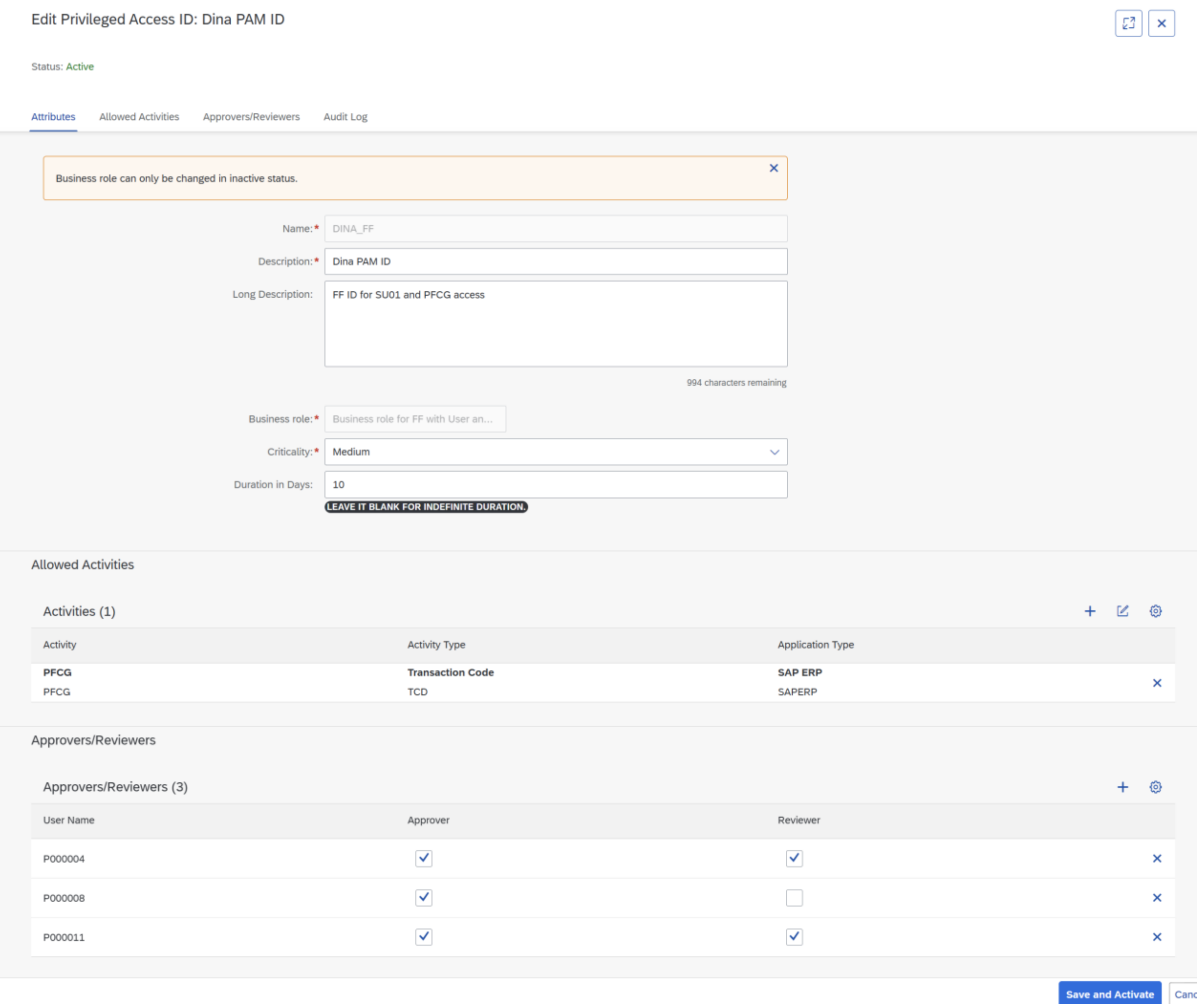
User Administration for all systems
Business Role: User Administration
Business process: Basis
0 Risks
3 Access
0 Users

Functionality Around Business Roles – Privilege Access Management

Only Business Roles can be assigned to PAM Users.

This reduces the number of PAM users to be set up tremendously.

For system opening and closing, you will need to set up only 1 PAM user with the Business Role that contains the system opening/closing access for all systems required.



Edit Privileged Access ID: Dina PAM ID

Status: Active

Business role can only be changed in inactive status.

Name:*	DINA_FF
Description:*	Dina PAM ID
Long Description:	FF ID for SU01 and PFCG access
	994 characters remaining
Business role:*	Business role for FF with User an...
Criticality:*	Medium
Duration in Days:	10
	LEAVE IT BLANK FOR INDEFINITE DURATION.

Allowed Activities

Activities (1)

Activity	Activity Type	Application Type
PFCG PFCG	**Transaction Code** TCD	**SAP ERP** SAPERP

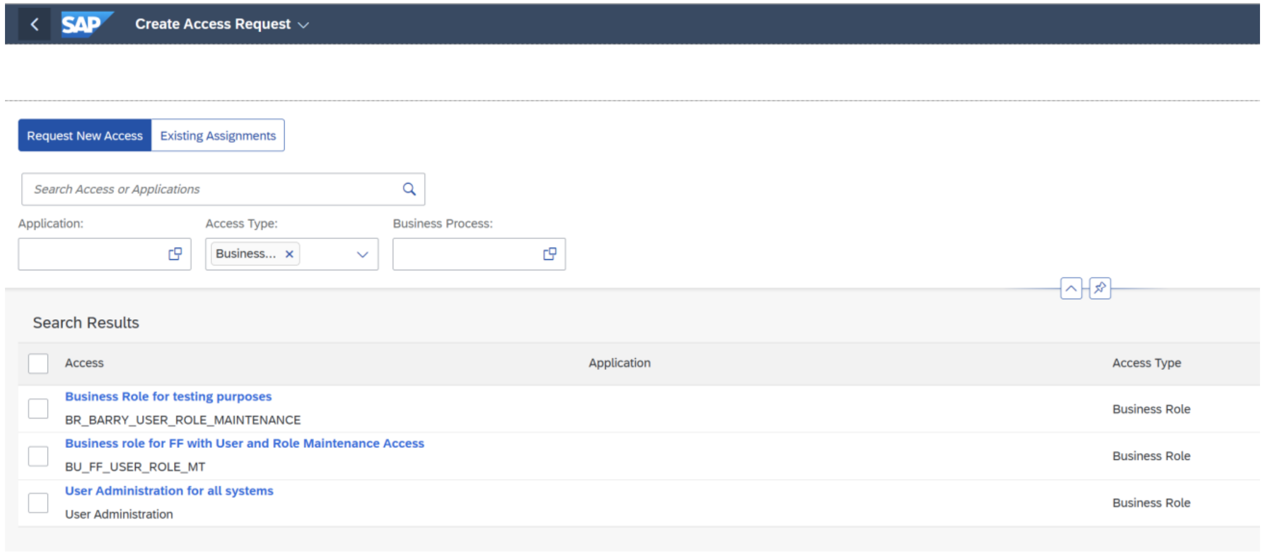
Approvers/Reviewers

Approvers/Reviewers (3)

User Name	Approver	Reviewer
P000004	☑	☑
P000008	☑	□
P000011	☑	☑

Functionality Around Business Roles – Access Request

When creating an Access Request, you can select Business Roles instead of having to select multiple roles/access across multiple systems.



Application:

Access Type: Business...

Business Process:

Search Results

□	Access	Application	Access Type
□	Business Role for testing purposes BR_BARRY_USER_ROLE_MAINTENANCE		Business Role
□	Business role for FF with User and Role Maintenance Access BU_FF_USER_ROLE_MT		Business Role
□	User Administration for all systems User Administration		Business Role

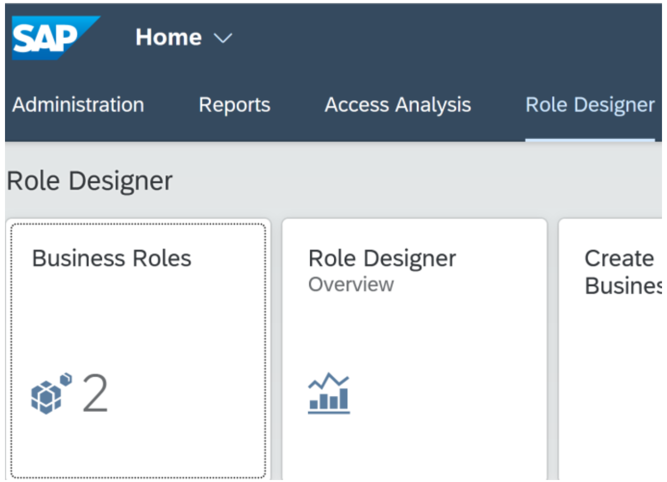
Technical Setup of a Business Role

You can either set up Business Roles manually or via utilizing the Role Mining capabilities.

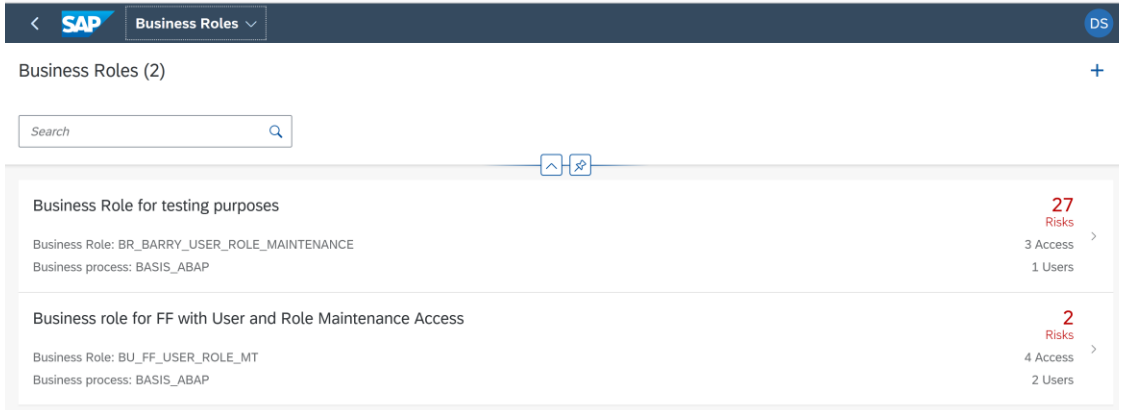
On the next slides, we will cover the manual setup of Business Roles.

Technical Setup of a Business Role – Manual Process

Click on “Business Roles” in section “Role Designer.”



Either select the Business Role you want to change or “+” to add a new Business Role.



Business Roles (2)

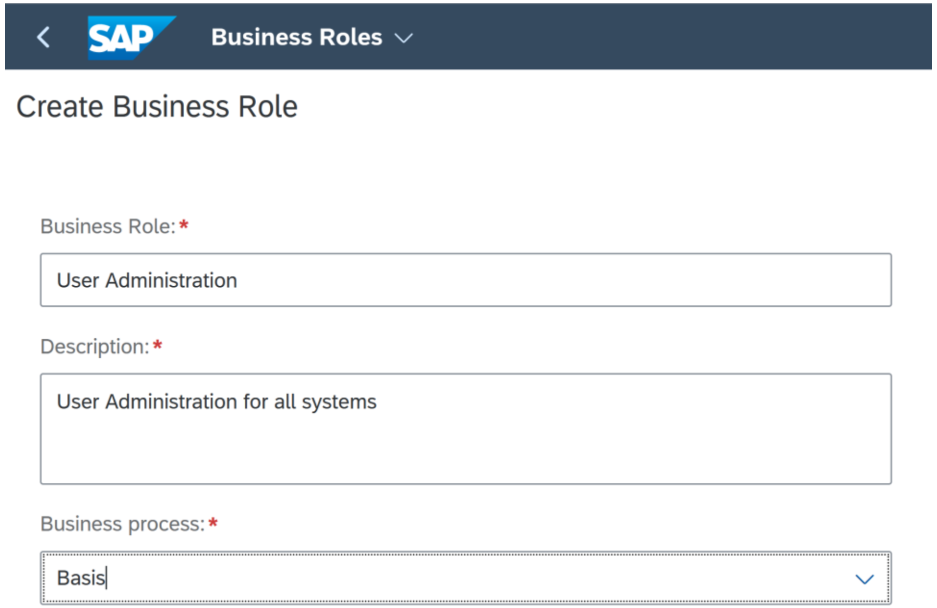
Business Role for testing purposes
Business Role: BR_BARRY_USER_ROLE_MAINTENANCE
Business process: BASIS_ABAP
27 Risks
3 Access
1 Users

Business role for FF with User and Role Maintenance Access
Business Role: BU_FF_USER_ROLE_MT
Business process: BASIS_ABAP
2 Risks
4 Access
2 Users

Technical Setup of a Business Role – Manual Process

Business Role Name:
The definition of the role name is very critical. Instead of using technical names as done in the back-end systems, it is essential that NON-technical names are used here. Please note that the end-users will in the end be the ones selecting the roles. They need to understand the name of the role, it therefore must reflect the language used in your company.

Technically the name can contain Numbers, Letters, spaces, and underscores



Create Business Role

Business Role: * User Administration

Description: * User Administration for all systems

Business process: * Basis

The Description should also contain Business Language. Both Role Name and Description are searched when requesting a role.

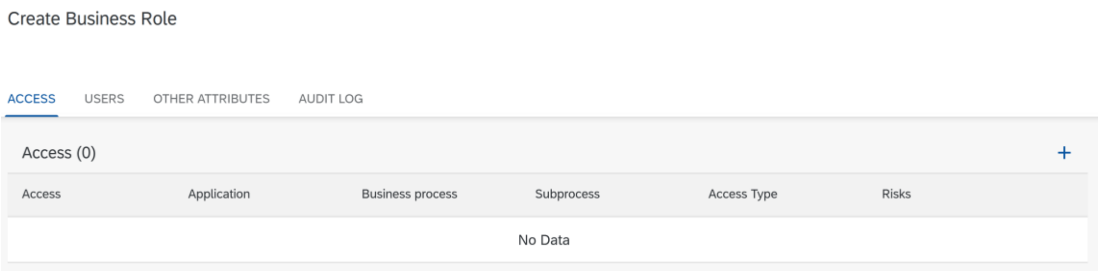
The assignment of the Business role to the right Business Process eases searching for the right role.

Technical Setup of a Business Role – Manual Process

Access:

In this step, you will select the role /access required for this Business role.

Click on “+” to select the roles / access

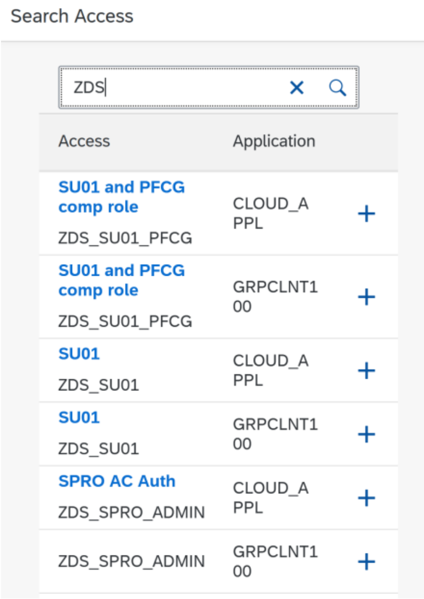


Create Business Role

Access (0) +

Access	Application	Business process	Subprocess	Access Type	Risks
No Data					

Search for the roles/access you want to include in the business role and select by clicking on “+”



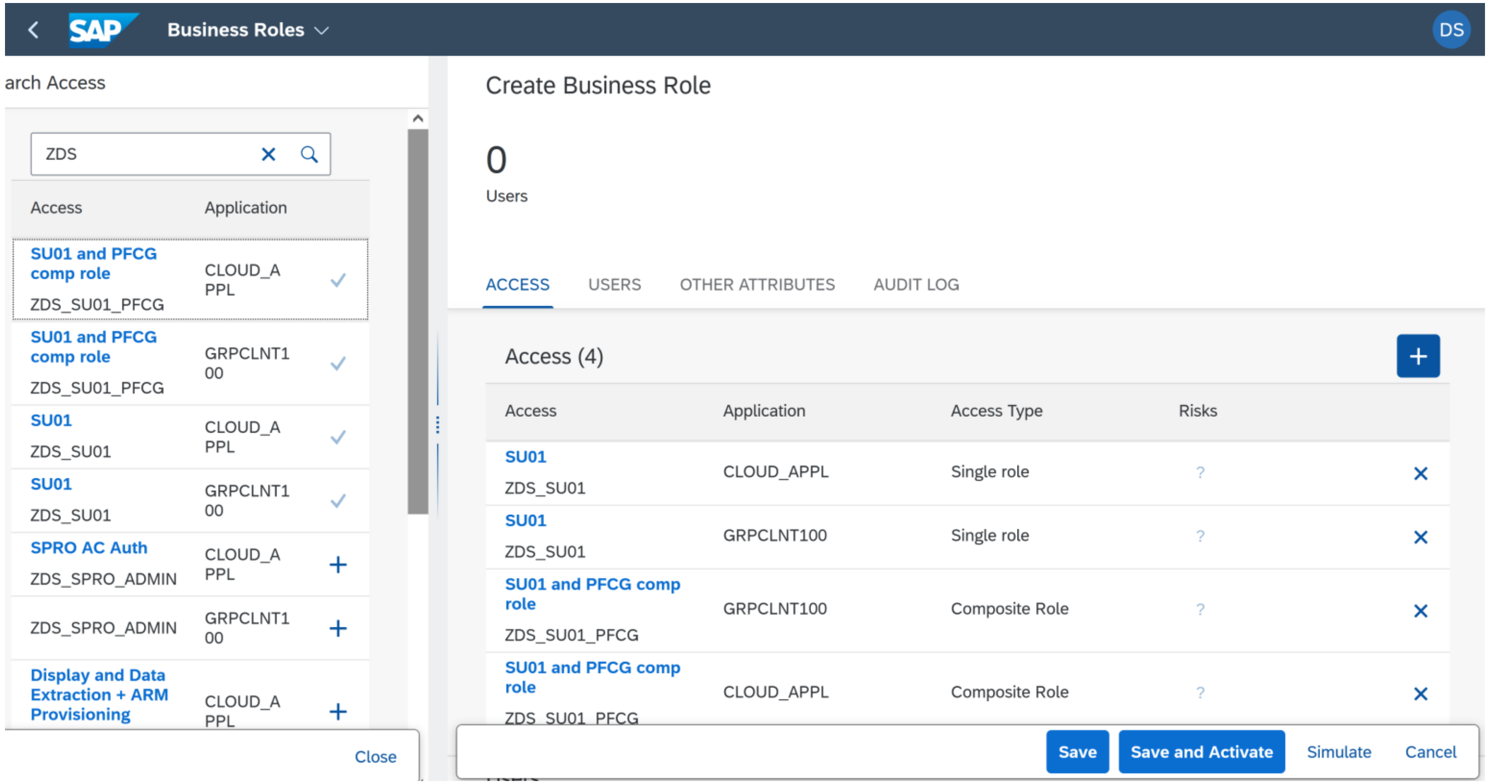
Search Access

ZDS

Access	Application	
SU01 and PFCG comp role ZDS_SU01_PFCG	CLOUD_APPL	+
SU01 and PFCG comp role ZDS_SU01_PFCG	GRPCLNT100	+
SU01 ZDS_SU01	CLOUD_APPL	+
SU01 ZDS_SU01	GRPCLNT100	+
SPRO AC Auth ZDS_SPRO_ADMIN	CLOUD_APPL	+
ZDS_SPRO_ADMIN	GRPCLNT100	+

Technical Setup of a Business Role – Manual Process

Once you are done with your selection, you can click on “Simulate.”



Access	Application	
SU01 and PFCG comp role ZDS_SU01_PFCG	CLOUD_APPL	✓
SU01 and PFCG comp role ZDS_SU01_PFCG	GRPCLNT100	✓
SU01 ZDS_SU01	CLOUD_APPL	✓
SU01 ZDS_SU01	GRPCLNT100	✓
SPRO AC Auth ZDS_SPRO_ADMIN	CLOUD_APPL	+
ZDS_SPRO_ADMIN	GRPCLNT100	+
Display and Data Extraction + ARM Provisioning	CLOUD_APPL	+

Access	Application	Access Type	Risks	
SU01 ZDS_SU01	CLOUD_APPL	Single role	?	✕
SU01 ZDS_SU01	GRPCLNT100	Single role	?	✕
SU01 and PFCG comp role ZDS_SU01_PFCG	GRPCLNT100	Composite Role	?	✕
SU01 and PFCG comp role ZDS_SU01_PFCG	CLOUD_APPL	Composite Role	?	✕

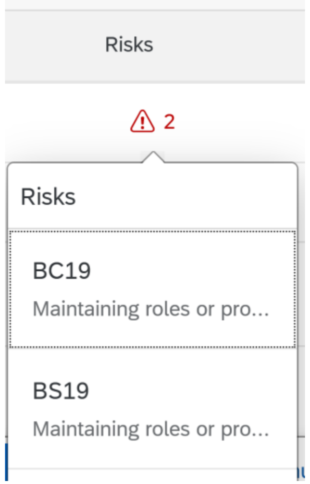
Technical Setup of a Business Role – Manual Process

Once you are done with your selection, you can click on “Simulate.”

The Risks will be displayed in Red.

Click on a Risk to see more details.

When you are not sure about the risk, Click on “Save” and discuss the risks with the responsible person from Business.



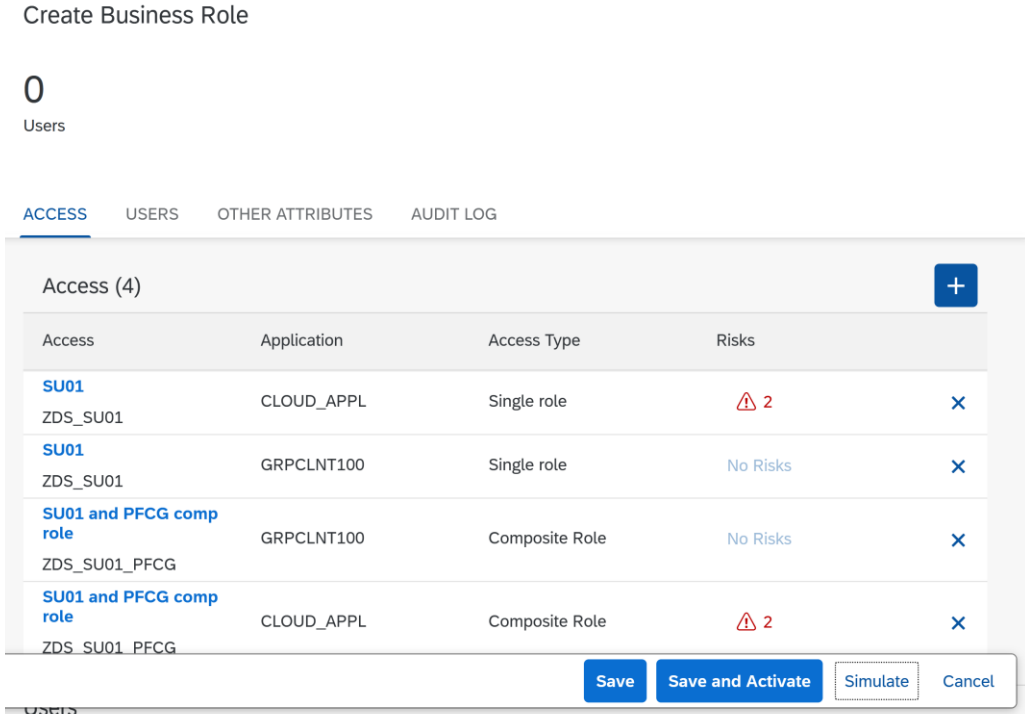
Risks

⚠ 2

Risks

BC19
Maintaining roles or pro...

BS19
Maintaining roles or pro...



Create Business Role

0
Users

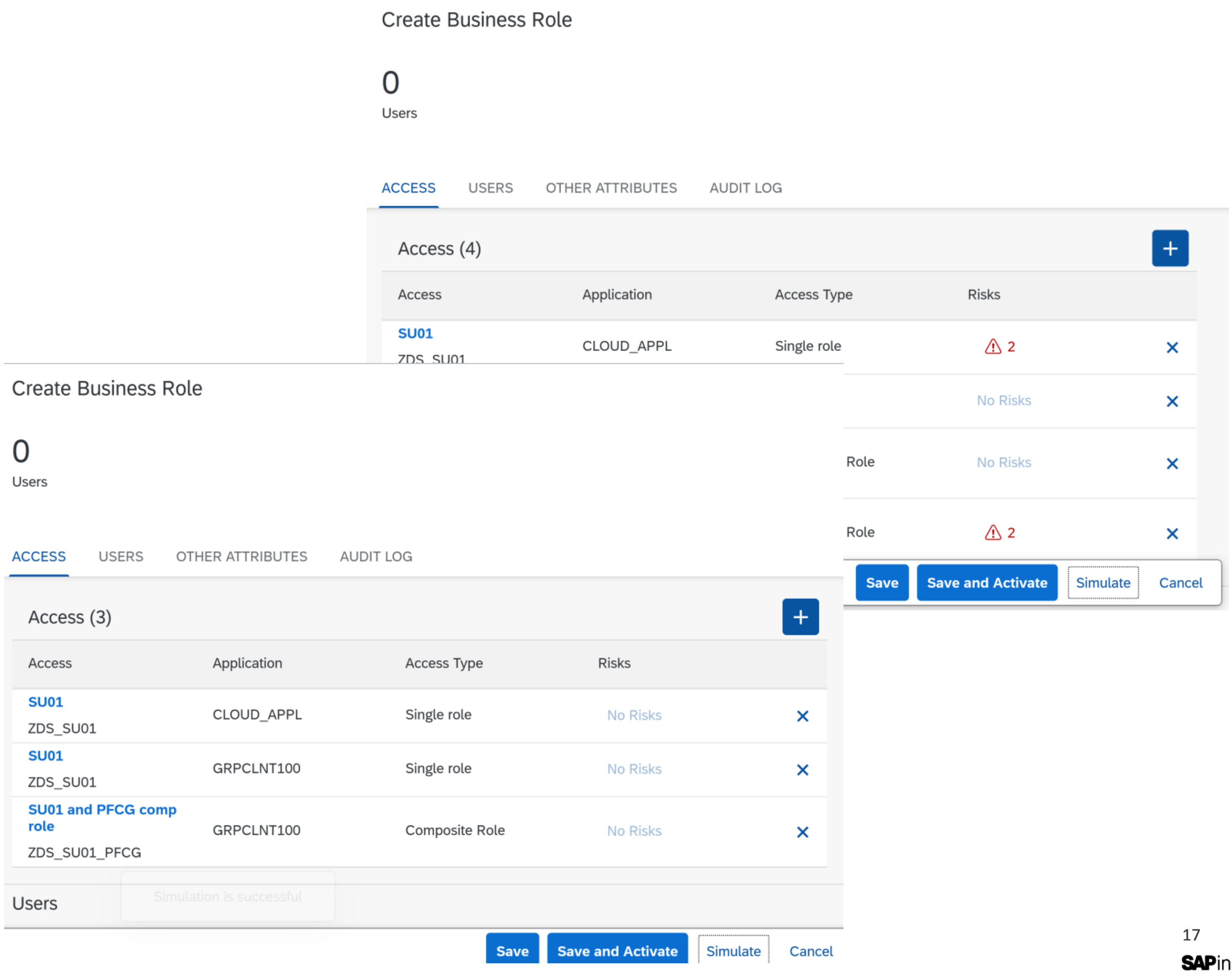
ACCESS | USERS | OTHER ATTRIBUTES | AUDIT LOG

Access (4)

Access	Application	Access Type	Risks
SU01 ZDS_SU01	CLOUD_APPL	Single role	⚠ 2
SU01 ZDS_SU01	GRPCLNT100	Single role	No Risks
SU01 and PFCG comp role ZDS_SU01_PFCG	GRPCLNT100	Composite Role	No Risks
SU01 and PFCG comp role ZDS_SU01_PFCG	CLOUD_APPL	Composite Role	⚠ 2

Technical Setup of a Business Role – Manual Process

You can remove roles that cause risks by clicking on “X” and run the Simulation again.



Create Business Role

0
Users

ACCESS USERS OTHER ATTRIBUTES AUDIT LOG

Access (4) +

Access	Application	Access Type	Risks	
SU01 ZDS_SU01	CLOUD_APPL	Single role	⚠ 2	×
			No Risks	×
		Role	No Risks	×
		Role	⚠ 2	×

Save | Save and Activate | Simulate | Cancel

Create Business Role

0
Users

ACCESS USERS OTHER ATTRIBUTES AUDIT LOG

Access (3) +

Access	Application	Access Type	Risks	
SU01 ZDS_SU01	CLOUD_APPL	Single role	No Risks	×
SU01 ZDS_SU01	GRPCLNT100	Single role	No Risks	×
SU01 and PFCG comp role ZDS_SU01_PFCG	GRPCLNT100	Composite Role	No Risks	×

Users

Simulation is successful

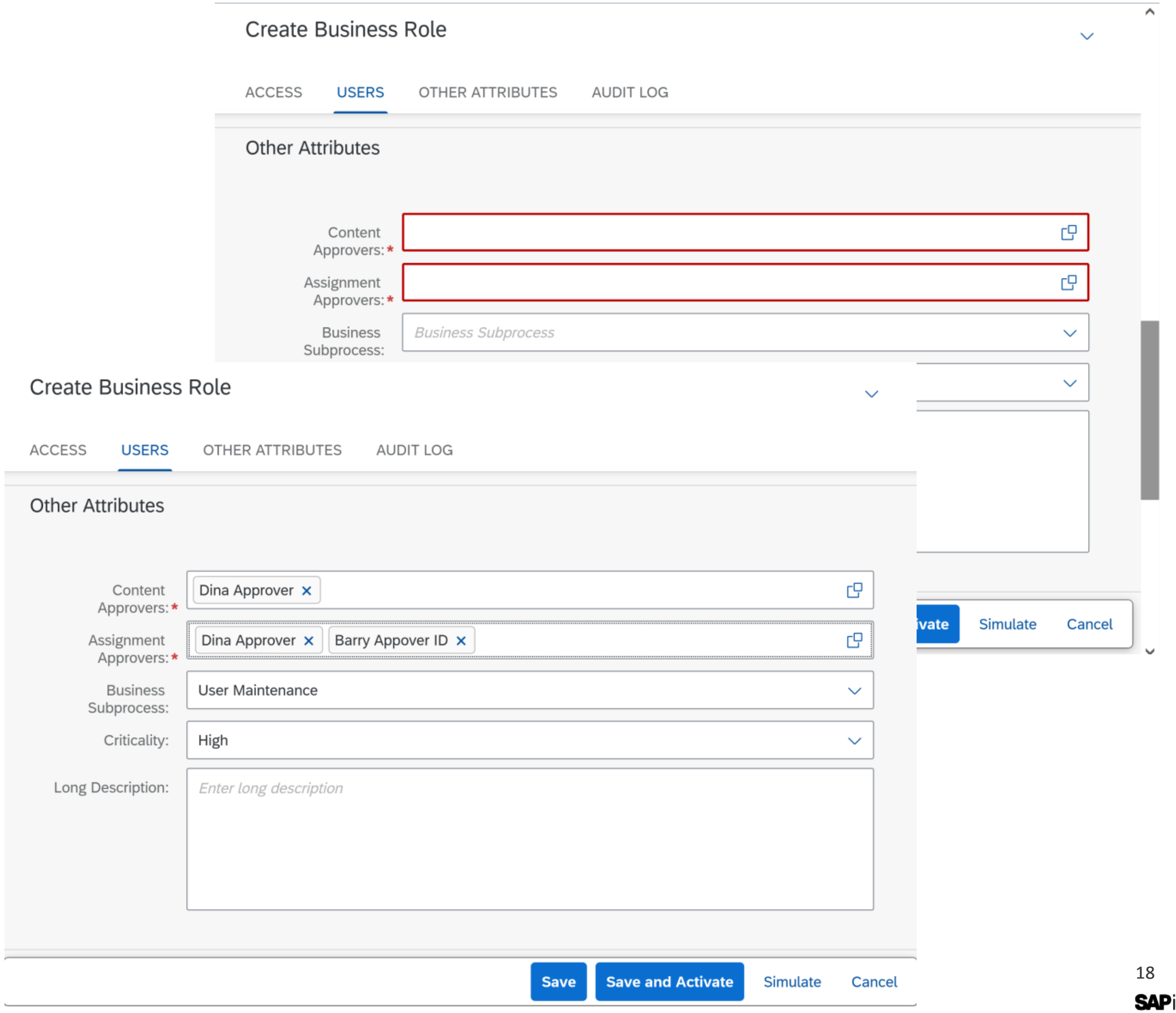
Save | Save and Activate | Simulate | Cancel

Technical Setup of a Business Role – Manual Process

Please define the:

- Content Approver(s): People responsible for the content of the Business Role and Approvers in case the access of a Business role is changed.
- Assignment Approver(s): People responsible for approving the assignment of the Business Role to users (in Access Request workflows).

Click on “Save” or “Save and Activate” when you want to make this Business Role visible in Access Request.



Create Business Role

ACCESS | USERS | OTHER ATTRIBUTES | AUDIT LOG

Other Attributes

Content Approvers: *

Assignment Approvers: *

Business Subprocess: Business Subprocess

vate | Simulate | Cancel

Create Business Role

ACCESS | USERS | OTHER ATTRIBUTES | AUDIT LOG

Other Attributes

Content Approvers: * Dina Approver ×

Assignment Approvers: * Dina Approver × Barry Appover ID ×

Business Subprocess: User Maintenance

Criticality: High

Long Description: Enter long description

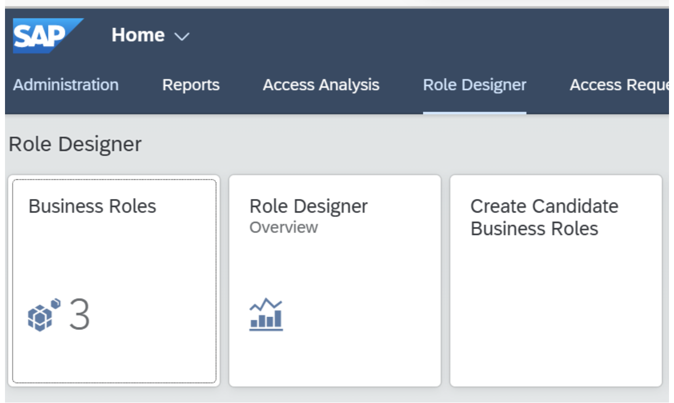
Save | Save and Activate | Simulate | Cancel

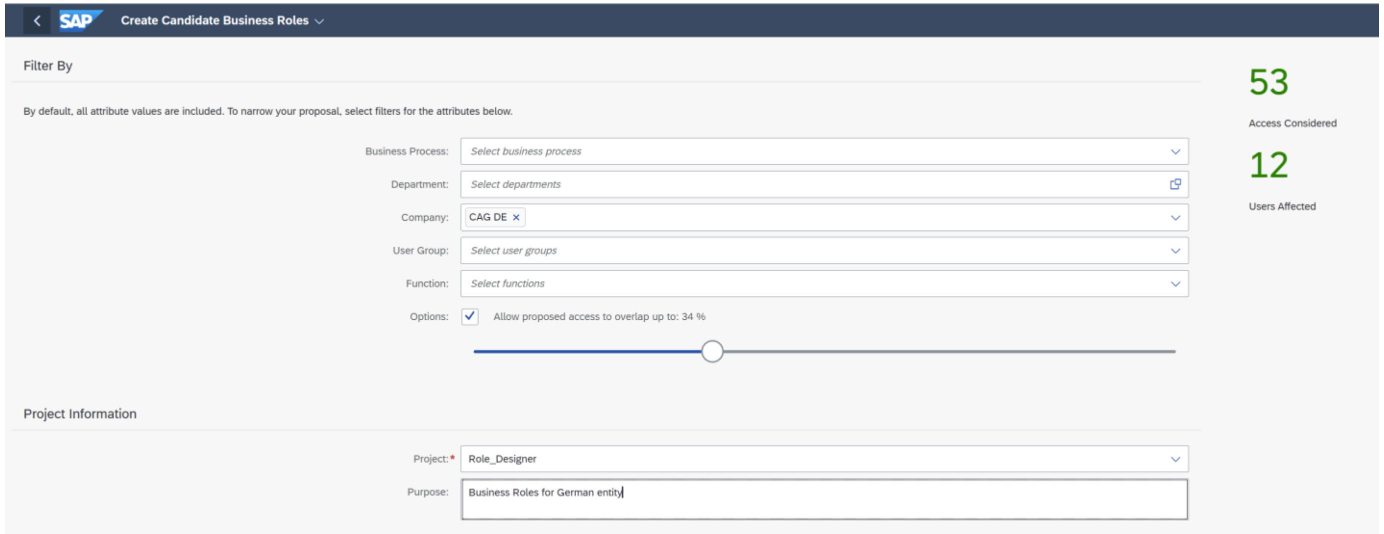
Technical Setup of a Business Role – Role Mining

Role Mining: How Does It Work?

In order to start the Role Mining, you can choose filters to analyze only certain

- **Users, by restricting**
  - Department
  - Company
  - User Group
- **Roles, by restricting**
  - Business Process
  - Function





Filter By

By default, all attribute values are included. To narrow your proposal, select filters for the attributes below.

Business Process: *Select business process*

Department: *Select departments*

Company: CAG DE ×

User Group: *Select user groups*

Function: *Select functions*

Options: ☑ Allow proposed access to overlap up to: 34 %

53

Access Considered

12

Users Affected

Project Information

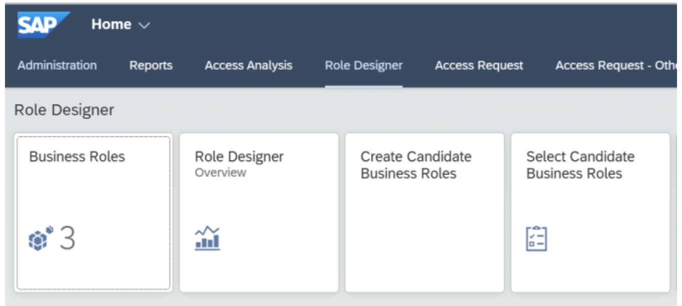
Project:* Role_Designer

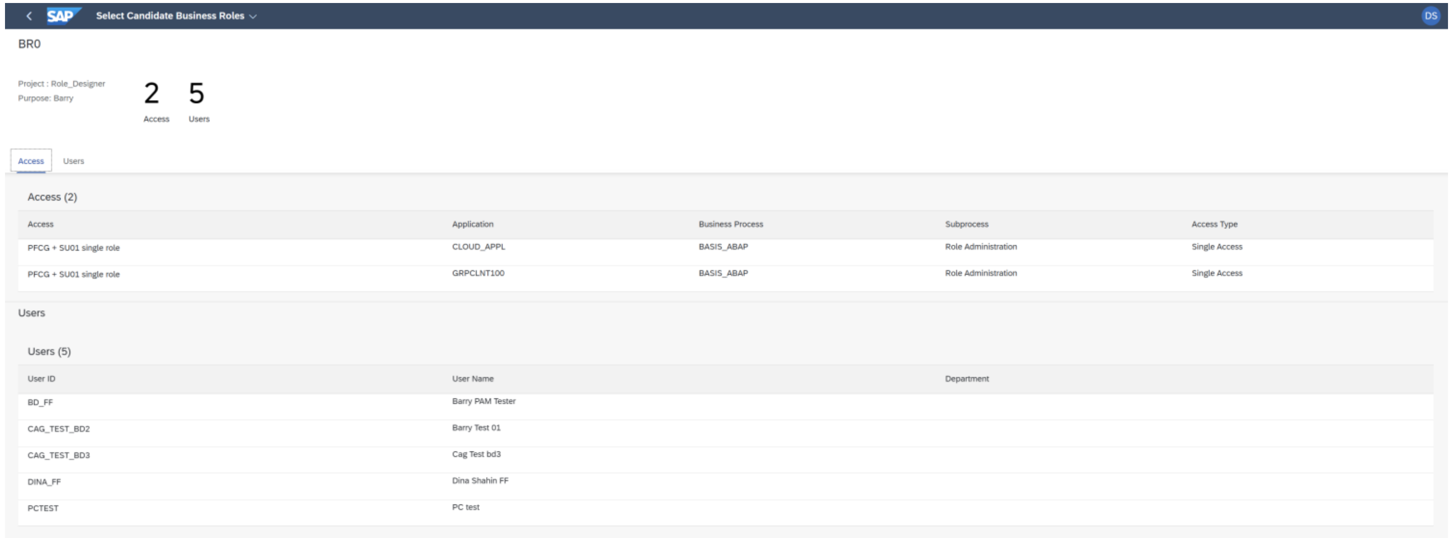
Purpose: Business Roles for German entity

Technical Setup of a Business Role – Role Mining

Depending on the restrictions done, IAG will determine the users and their role assignment and set up a candidate Business Role.

The roles can then be displayed in "Select Candidate Business Roles" and submitted to go through the Workflow.





BR0

Project : Role_Designer
Purpose: Barry

2 Access

5 Users

Access (2)

Access	Application	Business Process	Subprocess	Access Type
PFCG + SU01 single role	CLOUD_APPL	BASIS_ABAP	Role Administration	Single Access
PFCG + SU01 single role	GRPCLNT100	BASIS_ABAP	Role Administration	Single Access

Users

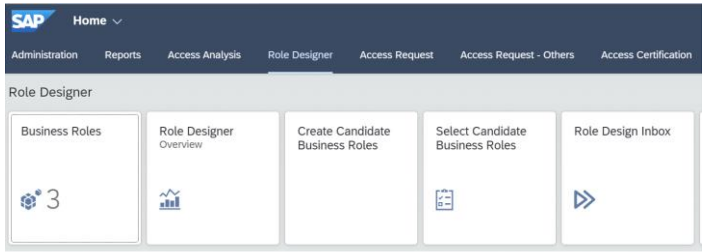
Users (5)

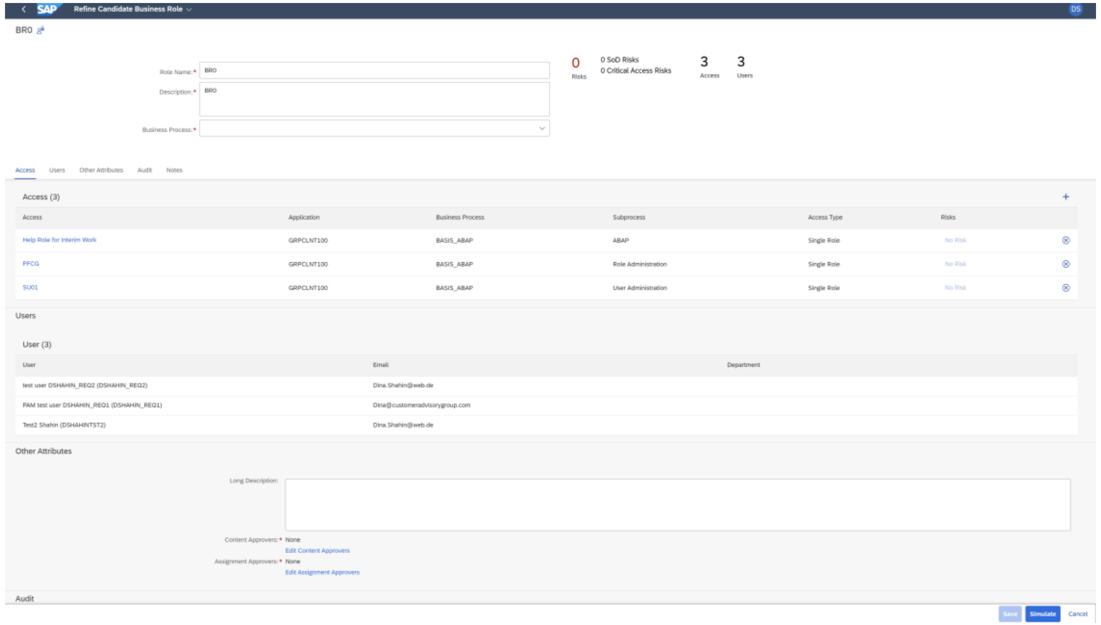
User ID	User Name	Department
BD_FF	Barry PAM Tester	
CAG_TEST_BD2	Barry Test 01	
CAG_TEST_BD3	Cag Test bd3	
DINA_FF	Dina Shahin FF	
PCTEST	PC test	

Technical Setup of a Business Role – Role Mining

The Workflow Covers 3 Stages:

- Refine: Here the Business Role Name is defined, roles are checked, and the approvers are defined. Once that is done, a Simulation checks for SoD issues in the role and the role can be saved.
- Activate: Once you are satisfied with your entries, activate the Business Role. The Candidate Business Role is then converted to a Business Role.
- Reconcile: The Business Role is reconciled.





BR0

Role Name:* BR0

Description:* BR0

Business Process:*

0 Risks | 0 SoD Risks | 0 Critical Access Risks | 3 Access | 3 Users

Access (3)

Access	Application	Business Process	Subprocess	Access Type	Risks
Help Role for Interim Work	GRPCLNT100	BASIS_ABAP	ABAP	Single Role	No Risk
PFCG	GRPCLNT100	BASIS_ABAP	Role Administration	Single Role	No Risk
SU01	GRPCLNT100	BASIS_ABAP	User Administration	Single Role	No Risk

Users

User (3)

User	Email	Department
test user DSHAHIN_REQ2 (DSHAHIN_REQ2)	Dina.Shahin@web.de	
PAM test user DSHAHIN_REQ1 (DSHAHIN_REQ1)	Dina@customeradvisorygroup.com	
Test2 Shahin (DSHAHINTST2)	Dina.Shahin@web.de	

Other Attributes

Long Description:

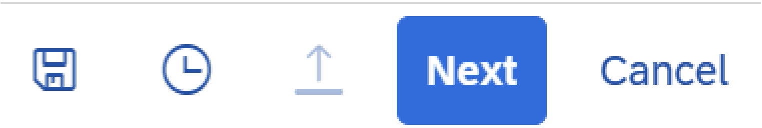
Content Approvers:* None
Edit Content Approvers

Assignment Approvers:* None
Edit Assignment Approvers

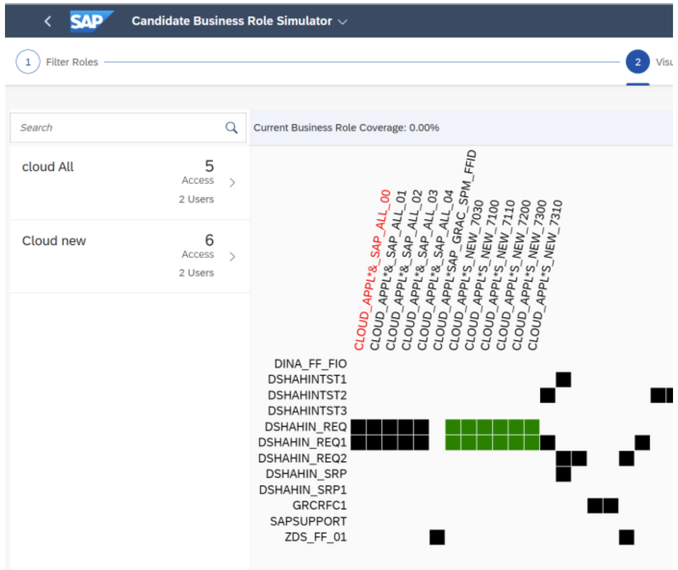
Audit

Technical Setup of a Business Role – Role Mining

Once you are done, save your changes and proceed by clicking the Next button.



Once that is done, the changes go through a workflow with following actions:



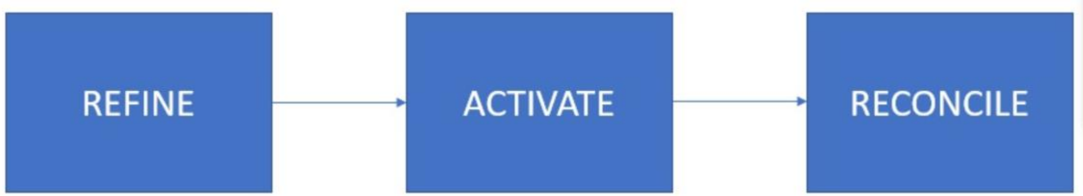
Current Business Role Coverage: 0.00%

cloud All 5 Access 2 Users

Cloud new 6 Access 2 Users

CLOUD_APPL*&_SAP_ALL_00
CLOUD_APPL*&_SAP_ALL_01
CLOUD_APPL*&_SAP_ALL_02
CLOUD_APPL*&_SAP_ALL_03
CLOUD_APPL*&_SAP_ALL_04
CLOUD_APPL*SAP_GRAC_SPM_FFID
CLOUD_APPL*S_NEW_7030
CLOUD_APPL*S_NEW_7100
CLOUD_APPL*S_NEW_7110
CLOUD_APPL*S_NEW_7200
CLOUD_APPL*S_NEW_7300
CLOUD_APPL*S_NEW_7310

DINA_FF_FIO
DSHAHINTST1
DSHAHINTST2
DSHAHINTST3
DSHAHIN_REQ
DSHAHIN_REQ1
DSHAHIN_REQ2
DSHAHIN_SRP
DSHAHIN_SRP1
GRCRFC1
SAPSUPPORT
ZDS_FF_01



REFINE → ACTIVATE → RECONCILE

Steps and Effort to Implement a Business Role Concept

Whenever implementing Business Roles/Grouping Access in Roles, you will want to make sure that:

- The roles/access in the role are complete and correct
- Do not contain access that causes unwanted SoD issues
- Role Name reflects the purpose of the role in Business Language
- Description of the role is written in Business Language as well
- Correct Role Content and Assignment Approvers are assigned

Steps and Effort to Implement a Business Role Concept

Before starting to implement a Business Role Concept, an assessment has to be carried out regarding which Role/Access bundles to convert to Business Roles

Both the Security Team(s) as well as Business need to be involved in that step.

- Business can point out larger departments/entities where people have the same access or require the same access.
- Security Teams can analyze huge clusters of the same Access given to bigger groups of users.

Why is this step required?

In a Proof of Concept, you can cover smaller groups of people to verify that that the Business Role Concept works.

However, when you want to implement Business Roles, it makes sense to start with Business Roles that affect bigger entities of your company.

Steps and Effort to Implement a Business Role Concept

Discuss the strategy you want to use when collecting the Role/Access Data for Business Roles.

Depending on your systems and data, the strategy to implement Business Roles can differ.

- **Manual Role Implementation**
  - Must be used when no user data is in place (e.g., a new system is being introduced in your company)
  - Must be used when old systems are replaced by new systems

- **Role Mining**
  - Can be used when user access data is in place

Steps and Effort to Implement a Business Role Concept

Collection of Data

- **Manual Role Implementation**
  - Both Business and Security Teams are involved in this step.
  - Business must provide the information which access must go into a Business Role.
  - Security has to translate the information into roles/access.

- **Role Mining**
  - Both Business and Security Teams are involved in this step.
  - Security will provide the Candidate Business Roles based on the approach agreed on before.
  - Business has to check whether the access is correct and complete and report missing access.

Steps and Effort to Implement a Business Role Concept

Implementation of Business Roles

- **Manual Role Implementation**
  - IAG Security Team is involved in this step.
  - The team must set up the new Business Roles, run a risk analysis and discuss the outcome with Business.

- **Role Mining**
  - The Implementation of the Business Roles is covered in the Workflow and is therefore finished once the Business Roles are activated and reconciled.

Pros and Cons of Implementing a Business Role Concept

Whenever implementing Business Roles/Grouping Access in Roles, you will want to make sure that:

- The roles/access in the role are complete and correct
- Does not contain access that causes unwanted SoD issues
- Role Name reflects the purpose of the role in Business Language
- Description of the role is written in Business Language as well
- Correct Role Content and Assignment Approvers are assigned

Pros and Cons of Implementing a Business Role Concept

As you can easily see setting up Business Roles requires a lot of work and participation of the Security Team(s) and Business:

Pros:

- The work effort can pay off when you select Business Roles/Role Groupings that will be assigned to larger groups of people.
- The work effort can pay off when you create Business Roles/Role Groupings for positions/jobs that require complex access to multiple systems.
- Cleaning up of users that have accumulated too much access over the years.
- Ongoing Administration: Changes of access can be provisioned/de-provisioned centrally via a Business Role change.

Pros and Cons of Implementing a Business Role Concept

As you can easily see setting up Business Roles requires a lot of work and participation of the Security Team(s) and Business.

Cons:

- Too much effort for smaller companies/departments/entities
- Technical Challenges: Switching to Business Roles requires more work at the beginning for the Security Team when creating users (e.g., give the user the same access as person XYZ)
- End-User Impact: Training of Business Users about what roles to select when requesting access.

Pros and Cons of Implementing a Business Role Concept

Pros and Cons:

- Technical Challenges: Cleaning up of roles/access with SoD issues
- Technical Challenges: Cleaning up of roles/access with unwanted critical access
- Technical Challenges: Business needs to learn what access roles/access contains
- Technical Challenges: Business Roles need to be updated when new systems are set live and old systems are de-provisioned.

Wrap Up

There is no one answer on whether to implement Business Roles or not. The decision can depend on the size of your end-users in different departments/entities and the complexity of your system landscape.

Implementing Business Roles for your company does not mean that you have to cover each and every case with Business Roles.

When implementing Business Roles, the strategy is very important. Invest much time into finding the right strategy to reduce your investment in effort and manpower.

Key Points to Take Home

- **Define your approach before starting the implementation Business Roles**
- **Review your Role concept before starting the usage of Business Roles**
- **Analyze (SOD) your Roles before starting implementing Business Roles**
- **Consider the number of Business Roles that end-users have to request in order to be able to do their job**
- **Keep *all* roles clean and tidy, but especially the Business Roles to avoid**
  - Duplicate entries
  - Confusion about role content
  - Overflow of user master records regarding role assignment

Thank You! Any Questions?

Dina Shahin

https://www.linkedin.com/in/dshahin/

Please remember to complete your session evaluation.

SAPinsider

SAPinsider.org

PO Box 982Hampstead, NH 03841

SAPinsider comprises the largest and fastest growing SAP membership group worldwide, with more than 600,000 members across 205 countries.