The SAP "Business Role" Concept – What It Can Do to Enhance Your Security Compliance Program.

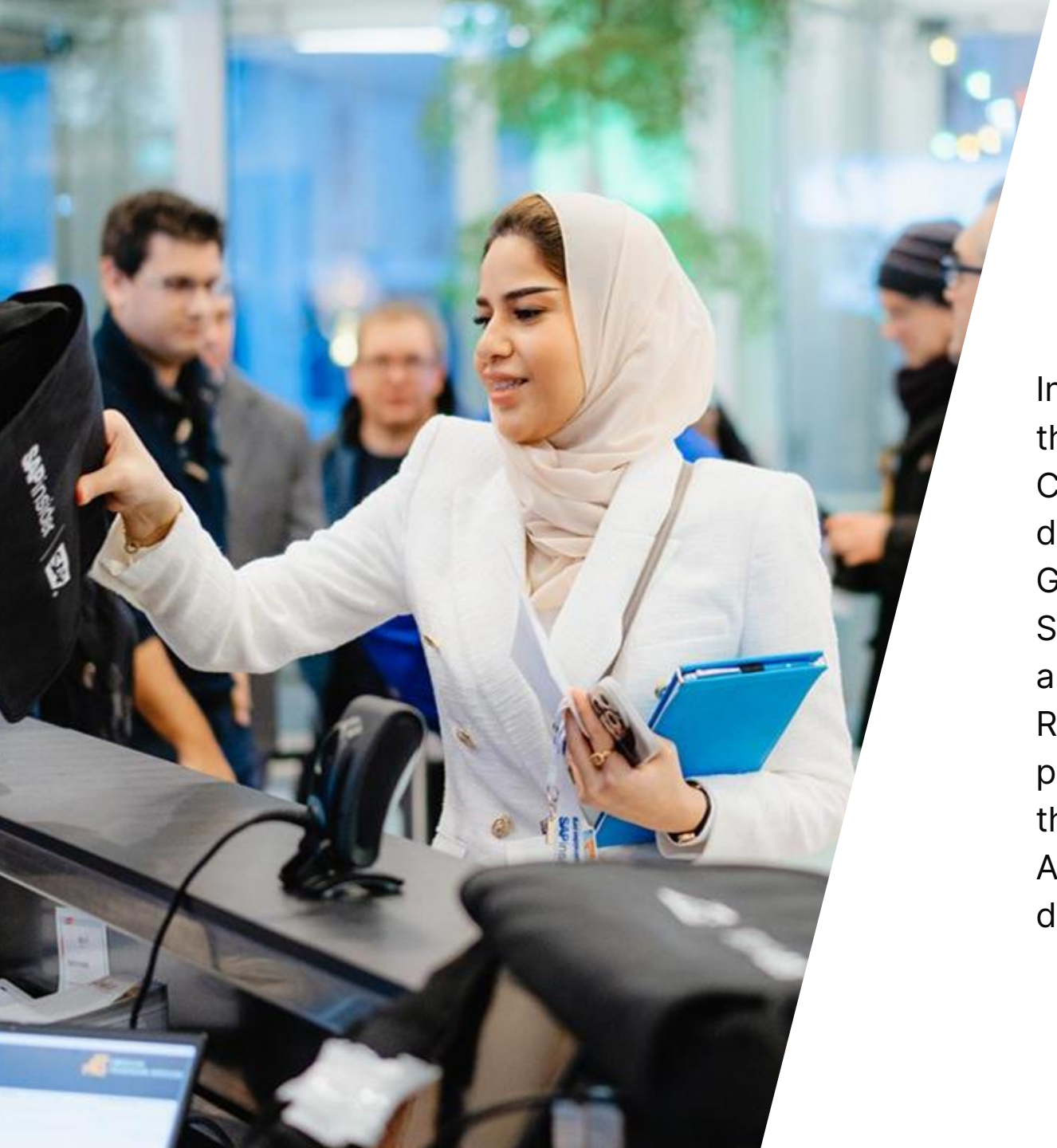
James E. Roeske, CEO
Customer Advisory Group

Gabriel Perez, Senior GRC Customer Advisor
Customer Advisory Group

Las Vegas

2024

SAPinsider



In This Session

In this session we will conduct a detailed examination of the Business Role concept in GRC Access Control and SAP Cloud Identity Access Governance. We will take a deep dive look into the Security structure concept of an SAP GRC Business Role as well as the specific functionality that SAP GRC Access Control and IAG provides to implement and support the creation and maintenance of Business Roles, SoD analysis of Business Roles, and the request and provisioning process all from the perspective of simplifying the SAP security process for end users and Administrators. This session will provide fact-based Demo driven insight into how GRC Business Roles operate.

In This Session

1. Understand the concept of what a Business Role is in Security and the definition it has within the SAP GRC Access Control system. This includes technical structure or lack-there-of in SAP PFCG. How BRM plays a significant role in the concept and technical architecture of a Business Role

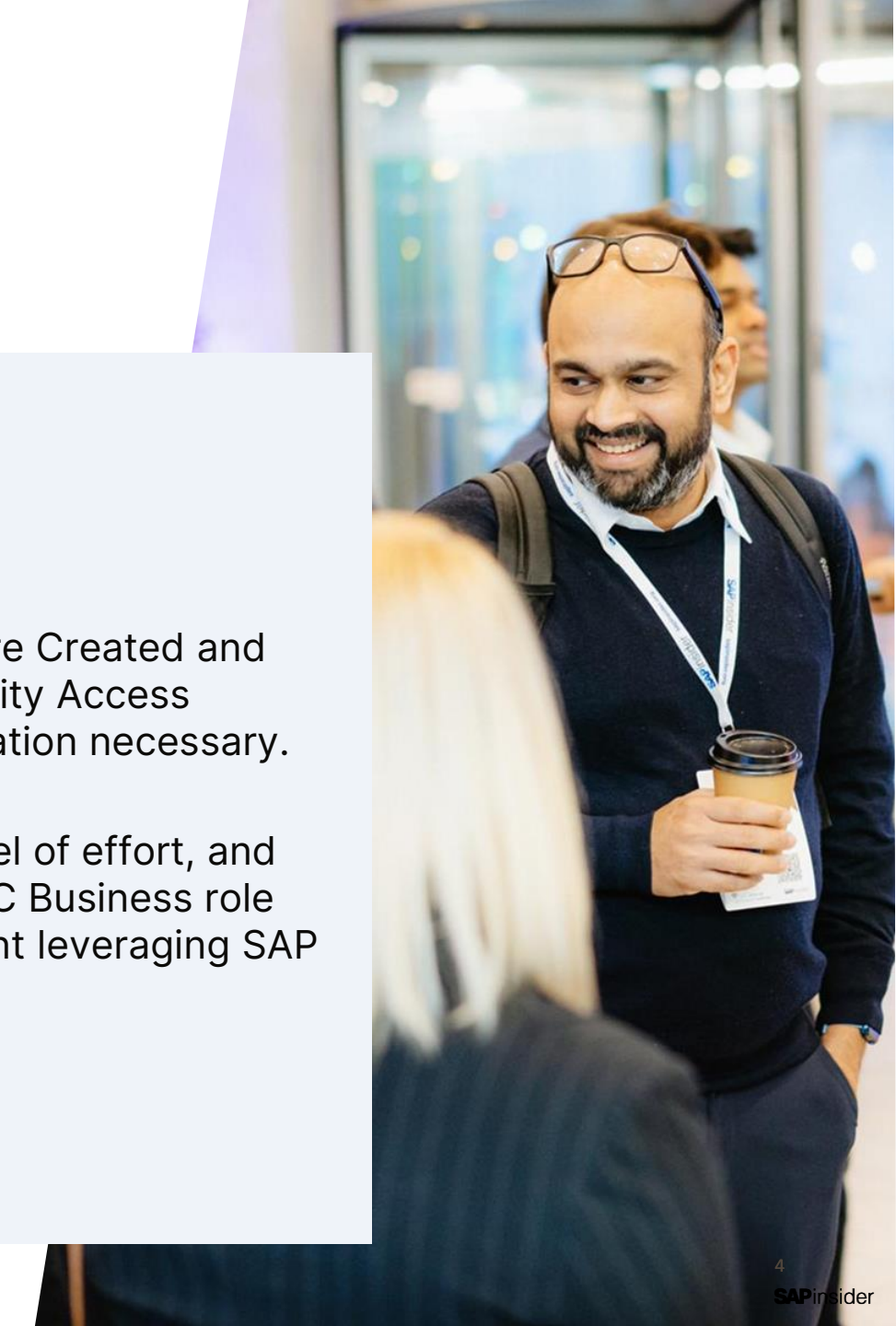
2. Examine the technical setup and functionality around Business Roles in SAP GRC Access Control with a deep focus on ARA SoD analysis capabilities, ARM business role selection and provisioning, and especially on BRM for Business Role creation and maintenance.

3. Examine the pros and cons of implementing the Business Role concept based on technical structure, End user impact, and long-term administration to help Customers decide if Business Roles are right for them equipping customers with fact-based insight to create a project business case

In This Session (continued)

4. Present a Demo showing how Business roles are Created and Maintained in SAP GRC BRM & SAP Cloud Identity Access Governance and the associated basic configuration necessary.

5. Gain a detailed understanding of the steps, level of effort, and resources necessary to implement the SAP GRC Business role concept into an existing customer's environment leveraging SAP GRC Access Control to it's fullest



Session Agenda

1. Introduction and value proposition of Business Roles based on the challenges that customers are facing with the traditional SAP Security concepts being used today.
2. Explanation of how Business Roles are managed in SAP GRC and the functionality integration points for SoD analysis simplification, Role selection simplification, and audit trail reporting.
3. Demo of Business Role Creation and Maintenance in GRC Access Control 12.0 and SAP Cloud Identity Access Governance

BREAK

4. The good, the bad, and the ugly of Business Roles, and explanation of how these can be successfully used in a realistic, compliant, self-service driven security while highlighting their challenges and potential issues they can cause as well.
5. Cover implementation approach, effort, and steps to properly implement the Business Role concept into an existing customer environment.
6. Wrap up and questions.

1. Business Role Concept & Value Proposition

Introduction and value proposition of Business Roles based on the challenges that customers are facing with the traditional SAP Security concepts being used today.

The Prime Directive of a Security Administrator

“Make sure that people have the Right Access at the Right Time to perform their defined and essential job duties. Nothing More and Nothing Less!”

Sounds easy, right? Unfortunately, it is NOT!

There are many different factors that influence the ability of accomplishing this:
1.The complexity and size of your System Landscape. This includes all the systems your users need to access to perform their job duties. Single System, Cross System, Cross Platform etc.
2.The complexity, structure, and granularity of your security (SAP Role Structure, Naming conventions, number of Roles a person needs to come together to provide the access a person needs)
3.The Tools and processes you have established to allow people to request accesses, or to automatically update Access levels to change as people’s job duties change.

Security Workloads and Complexity are Increasing

"Back in the old days when I started in SAP I only had to worry about ONE R/3 Landscape (Dev, QA, and PRD). People would send me an email, or pick up the phone and call me to discuss a security issue. I would then "Fix it" by making a role change or assigning a new role to them. I knew all my roles and their basic content by heart!"

Times have changed!

"Now, I need to worry about ELEVEN different SAP Landscapes today with some users needing access to a combination or all eleven systems in volving 10-100 different roles. I also need to have everything documented for the Auditors, check for segregation of duty issues, assign Mitigations, obtain approvals for changes....and that is only in SAP, it does not include the new Cloud Applications we are in the process of implementing and and the Non-SAP systems that I need to administer!!!!"

Type of System	System	Client	Notes/Requirements	Type of System	System	Client	Notes/Requirements
ECC	PRD(1)(2)	700	(1) Tolerance level, (2) purchasing group	Solution Manager	SMD(6)		Production (6) Business Partner must be setup
	QAS	700			SMX		Development
	DEV	200 & 700		GRC	GRP		
	SND	700	Sandbox (limited to IT in RBAC)		GRD		
APO	APP			Fiori	GWP		
	APQ				GWQ	200	Client 200 on GWD box
	APD				GWD	100	
	APS		Sandbox (limited to IT in RBAC)	Enterprise Portal	EPP		
BW	BWP(3)		(3) Notification sent to training		EPQ		
	BWQ				EPD		
	BWD			DMF	DMP		IT only as part of RBAC
CRM	CRP(4)(5)		(4) Maintain parameters, (5) CRM exception for credentials – send credentials to CRM setup DL		DMQ		IT only as part of RBAC
					DMD		IT only as part of RBAC
	CRQ			BOBJ	BOBJP		Part of BW
	CRD				BOBJQ		Part of BW
BPC	BPC Prod		Provisioned through BW?		BOBJD		Part of BW
	BPC QA		Provisioned through BW?				
	BPC Dev		Provisioned through BW?				

The Evil Evolution of User Access and Role Design

- Security Admins Giveth Access, and Taketh Away! (Well, most of the time!)

- **It is very easy to give access.**
- Manager say they needed the Role, so we give it.

- **But not as easy to take it away.**
- Are they still using it, is it critical for their job?

What does the Term “Business Role” Actually Mean to you as an SAP Security Administrator?

This is what the SAP Security Dictionary definition says:

“A business role is a set of access rights that you can assign to multiple business users who perform similar business tasks.”

Now a Days the term “Business Role” is used in many many different ways! It is referenced both as a RBAC (Role Based Access Control) Security Design Concept as well as used when discussing SAP GRC or IDM Identity Management product functionality.

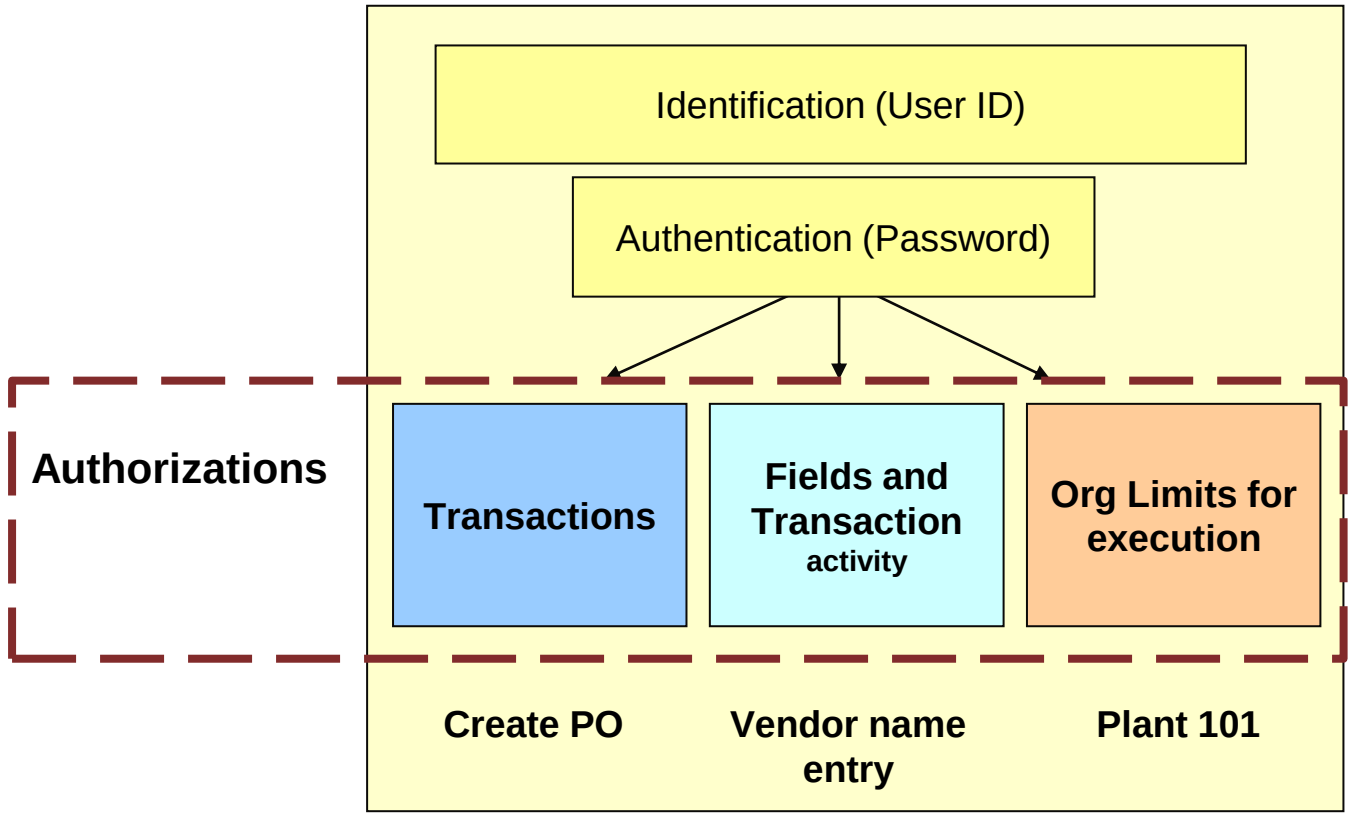
So which one is it, a Role design concept or an important piece of Security software functionality?

Actually, it’s both!

SAP Security 101

SAP Authorization Concept.

The Good Ol' Days of SAP ABAP Security.



Security Design 101 (Security Role Design)

It is then the Responsibility of Business Owners and Security Administrators to bundle these Authorizations together into logical groupings to give people access to do their jobs.

The ”Security Role” was born!

Roles types can vary in SAP:

- Profiles - place authorizations into one container
- Single Roles - place authorizations into one container
- Composite Roles - can be used to group multiple roles in a single system
- Derived roles are generated from a “master role” with desired number of organizational values so each can be assigned separately to control access to specific cost centers, purchasing orgs, or company codes.
- Business Roles can be used to group multiple roles across multiple systems
  - (New Type of Role, ONLY supported by SAP GRC Access Control and SAP Cloud Identity Access Governance)

Security Design 101 (Profiles)

- Profiles were the primary way to group authorizations up to SAP R/3 3.1G to group the authorizations
- The profiles were then assigned to users
- After SAP R/3 3.1G, roles a.k.a “Activity Groups” could be maintained
- But still SAP had to support profiles as well
- So for every role/activity group profiles were automatically generated
- The maintenance of roles/activity groups was performed with the SAP profile generator
- Whereas each and every authorization object and their values had to be manually inserted into profiles, the SAP profile generator automatically inserts the authorization objects for each transaction included in the role/activity group
- Only the mapping of transactions and their authorization objects and values has to be maintained once in SU24.

Security Design 101 (Roles)

Authorizations are not granted directly to the users. but are gathered in roles (called Activity Groups up to SAP R/3 release 4.6B)
Roles are also called Single Roles

Change role: Authorizations

Selection criteria | Manually | Open | Changed | Maintained | Organizational levels... | Information

Maint.: 0 Unmaint. org. levels 0 open fields, Status: Unchanged

SAP_BC_CLIENTCOPY	Client Copy	
Standard	Cross-application Authorization Objects	AAAB
Standard	Transaction Code Check at Transaction Start	S_TCODE
Maintained	Basis: Administration	BC_A
Maintained	Data Import for Client Copy	S_CLNT_IMP
Maintained	Authorization for file access	S_DATASET
Standard	Cross-Client Table Maintenance	S_TABU_CLI
Maintained	Table Maintenance (via standard tools such as SM30)	S_TABU_DIS
Standard	Table Maintenance (via standard tools such as SM30)	T_BE06004100
Activity	01, 02, 03	ACTVT
Authorization Group	SS	DICBERCLS
Maintained	Table Maintenance (via standard tools such as SM30)	T_BE06004101
Maintained	User Master Maintenance: User Groups	S_USER_GRP
Maintained	User Master Maintenance: Authorization Profile	S_USER_PRO
Standard	Basis - Development Environment	BC_C

Security Design 101 (Composite Role)

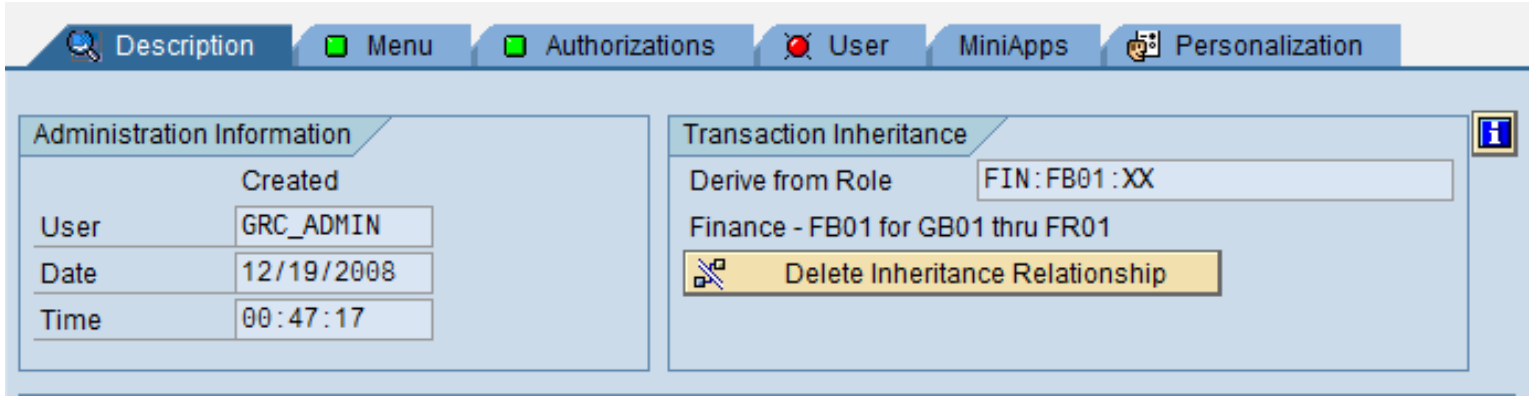
- Multiple single roles can be combined in composite roles
- The composite roles only contain single roles but no authorizations
- Composite Roles cannot contain other composite roles!

Description | Roles | Menu | User | Personalization

Role	Name	Target sys	Activ
SAP_SLD_ADMINISTRATOR	SAP_SLD_ADMINISTRATOR	user system	☑
SAP_XI_ADMINISTRATOR_ABAP	Exchange Infrastructure: Administratio	user system	☑
SAP_XI_ADMINISTRATOR_J2EE	Exchange Infrastructure: Administratio	user system	☑
SAP_XI_BPE_ADMINISTRATOR_ABA	Exchange Infrastructure: BPE Adminis	user system	☑
SAP_XI_DEMOAPP	Exchange Infrastructure: XI Demo Exa	user system	☑

Security Design 101 (Derived Roles)

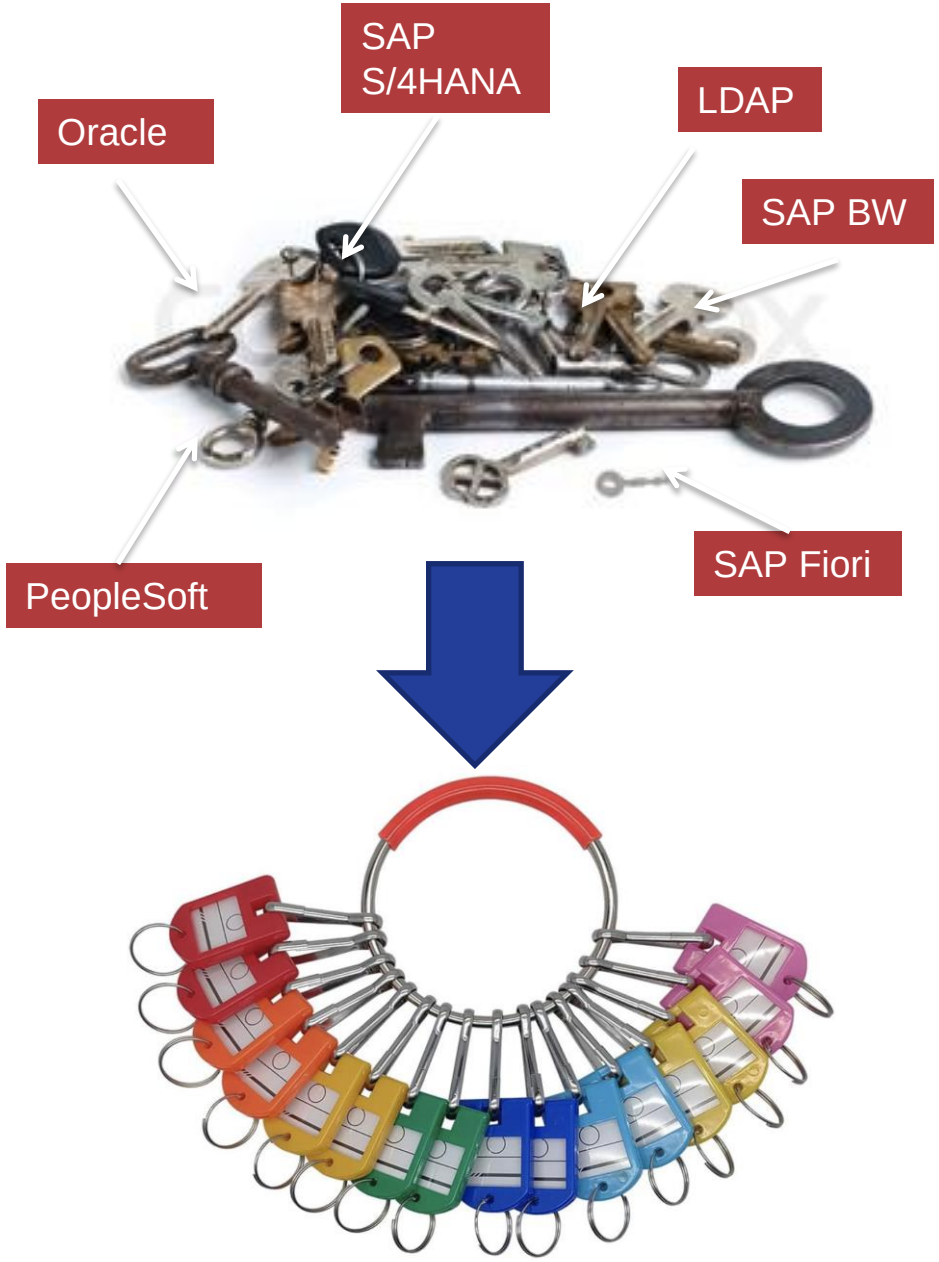
- When maintaining a role, the organization usually wants to grant the same functionality to different users for different entities (e.g., Plants)
- Instead of having to copy a role all over again and maintaining the Organizational Levels over and over again, the roles can be derived
- A role is chosen to be the master role
- From this role all entries will be handed down to the derived roles
- Only the Organizational Levels can be changed in the derived roles



Security Design 101 (Business Role)

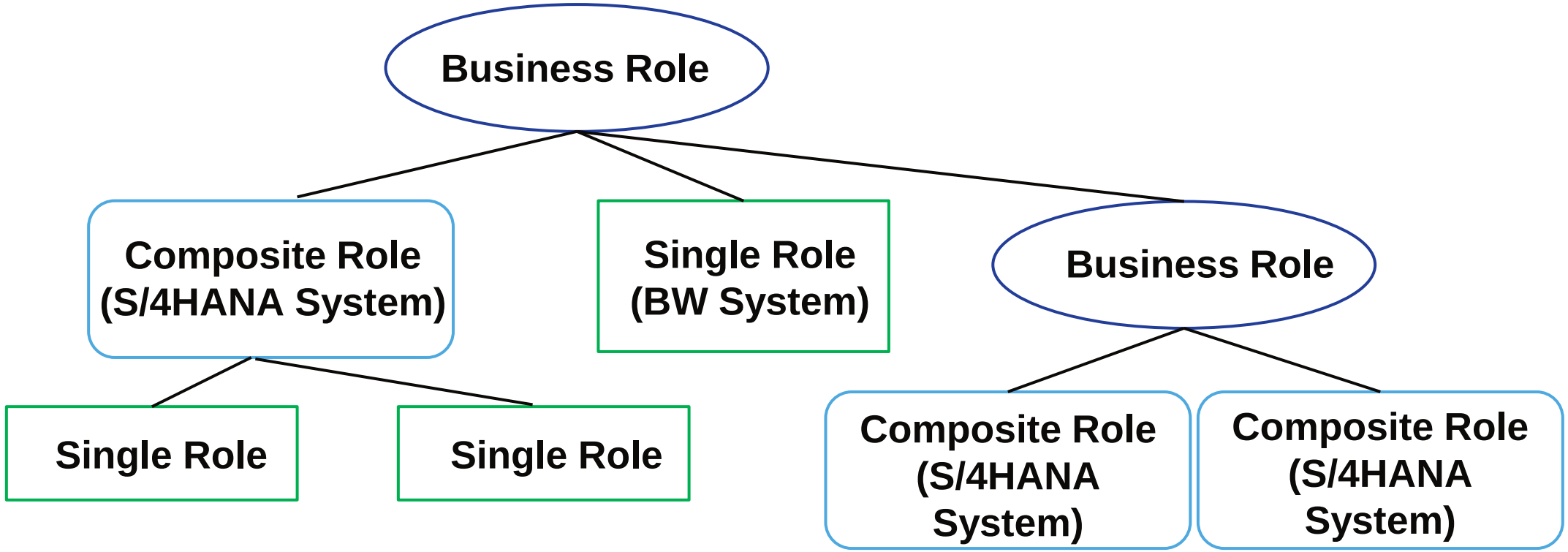
New Security Provisioning concept created by Identity Management applications and now supported by SAP GRC 10.

Largest Security container to group security privileges for multiple applications and multiple systems together under a single Business Role that can be provisioned to a User.



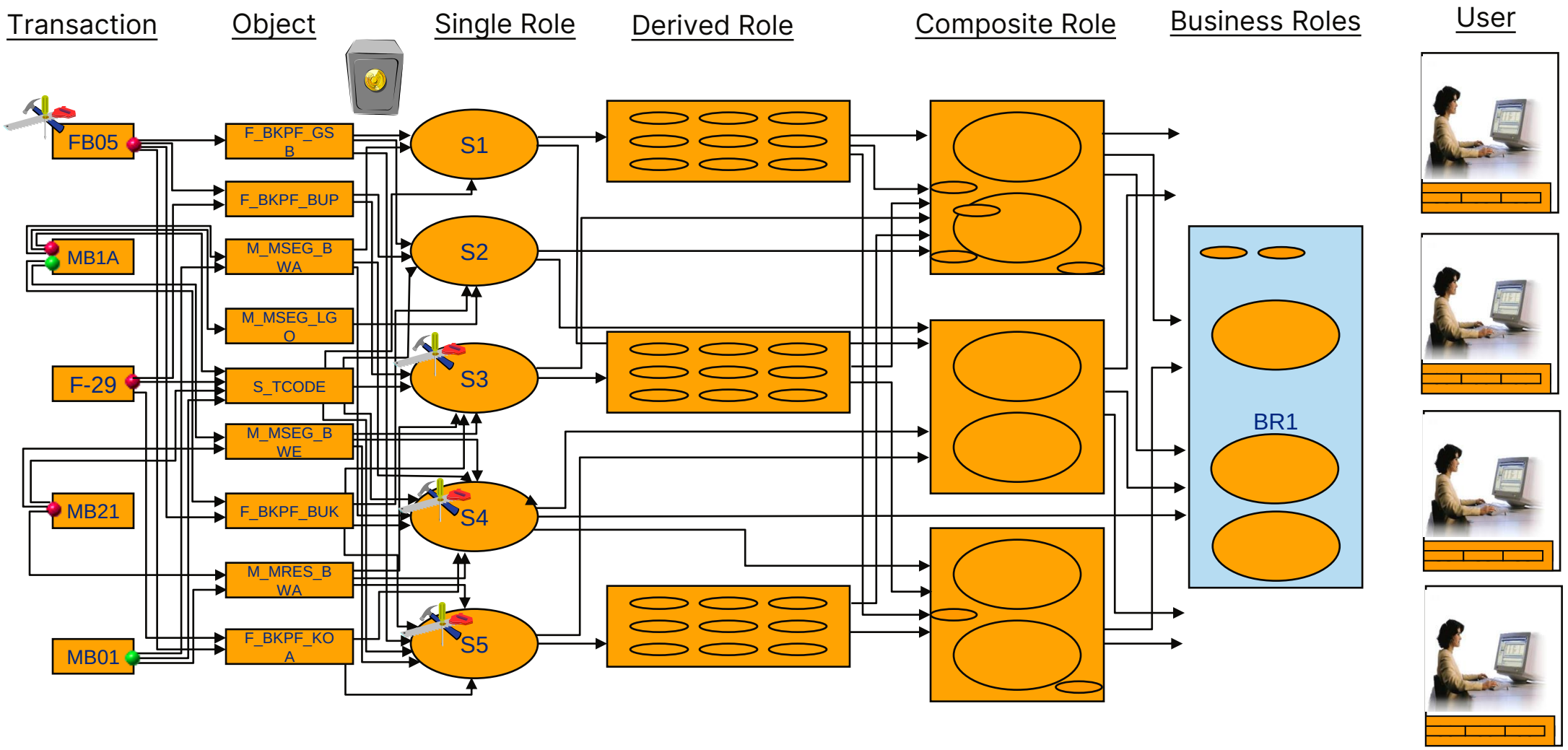
What is special about a Business Roles?

Basically, a Business Role is Like a “Cross System Composite” that bundles multiple roles together from multiple systems under a single usable and selectable name.



Business Roles Are Created, Maintained, and Managed ONLY in SAP GRC BRM. There is no direct link between a Business Role stored or captured outside of SAP GRC, including in PFCG or SU01.

Where do Business Roles Fit in?



There are a Wide Variety of Role Concepts. What Do You Have?

Customers can have some pretty extreme Role Concepts!

Authorization Concepts can vary between:

- One transaction code per role
  - Too much confusion when it comes to the content of a role
  - Too many roles per user

- One role per user
  - Too much functionality in a single role to cover all users executing the same job
  - No appropriate solution to cover exceptions

General Approaches to Security You Might Be Using Today

Tasked Based

- Divides roles by user activity or tasks

Position Based

- Divides roles by position that is held by user

Value based a.k.a "Enabler Roles"

- New term which provides a role which only contains organizational values to limit organizational access

Vendor Delivered Roles

- Roles delivered with the Software which contains prepopulated roles for AP Manager, AR Manager, etc.
- Becoming more prevalent with new Cloud applications
  - ***These type of Roles can contain significant inherent Segregation of Duty problems***

Role Design —
“The Perfect” Way Doesn’t Exist

Finding the right level of granularity is tough!

But Business Roles can be a mechanism to help put all the pieces together.

- Different concepts may apply for different systems
  - SAP S/4HANA vs. SAP Business Warehouse vs. Fiori vs. SuccessFactors etc.…
- Different concepts may apply for different modules
  - SAP Controlling vs. SAP Material Management
- Different concepts may apply for different entities
  - Different procedures in different SAP systems at the same company

Challenges — Security Role Design

Security design goal - Find the golden rule

- Allow users to perform their required tasks in the system
  - Without creating roles that are too huge
  - Give users what they need, not “a lot” of extras
  - Without creating too many Roles
- Keep it simple but secure

Create a security design and implementation strategy document

- Define naming conventions that are understood by Business Users
- Prepare role definitions with all pertinent details
- Develop role Best Practices for your scenario(s)

Incorporate role owners

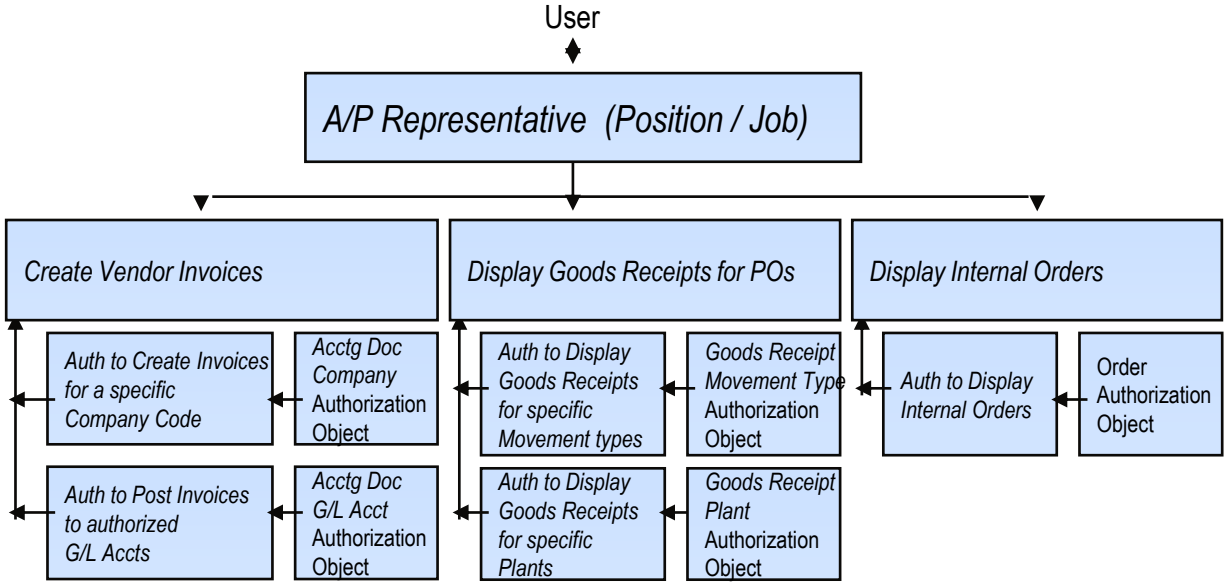
- They know what access is required at the different job levels
- They need to know the content of their roles
- Last but not least, they are responsible for the roles!

Example Business Role Design Concept

Business roles are an efficient way of managing roles in an organization and modeling them based on a job function

Each business role can represent a Job role or function and is associated to one or more related Technical Roles

- This Business Role contains all the authorizations that Accounts Payable Clerk needs to perform his activities
- Several Single/Composite roles may exist under this Business Roles
- These Single/Composite roles could exist from various systems (e.g., S/4HANA for daily tasks, BI for reporting, HR for timesheets)

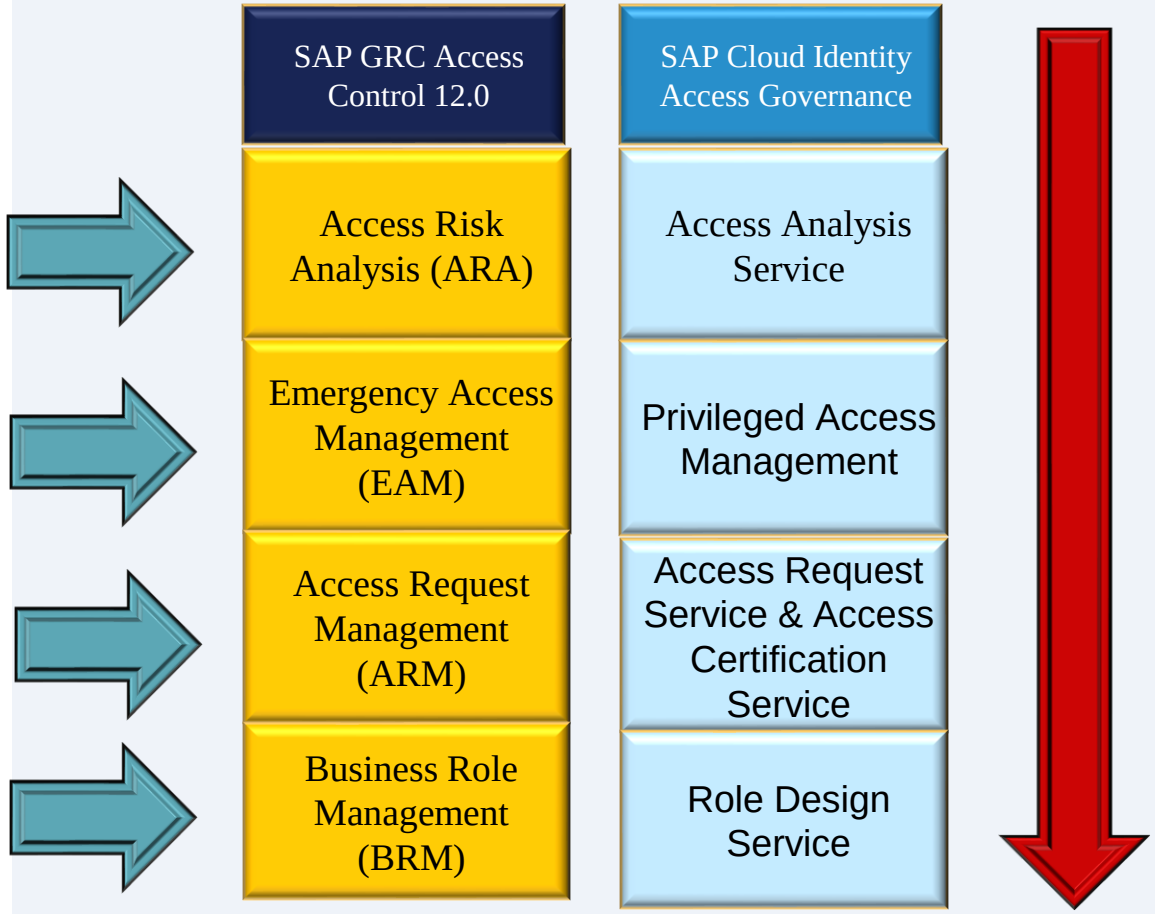


Business Roles in Terms of Software Functionality

Do you have SAP GRC 12.0 or SAP Cloud Identity Access Governance? Do you have the Business Role Management or IAG Role Design Service configured already?

- Most critical application for compliance related to SoD's. As well as very important for risk analysis to be integrated within other SAP Access Control components.
- Quick and easy to configure and get up and running. Can instantly solve outstanding audit points related to excessive access levels. Speedy return on investment.
- Key component for "Continuous Compliance" and enforcing proactive SOD checking rather than reactive. Primary mechanism for automating the provisioning process. This component will provide additional benefit AFTER the initial "Clean-up and mitigations" of SOD issues have been completed.
- Enables the enforcement of a consistent Role creation, maintenance and documentation process for Security Roles. Provides direct simulation and SOD checking to provide proactive SoD prevention during role development and maintenance.

BRM is usually the last to be Implemented by a Customer



2. Business Role Management and Integration Points

Explanation of how Business Roles are managed in SAP GRC and the functionality integration points for SoD analysis simplification, Role selection simplification, and audit trail reporting.

Managing Business Roles

Existing role concept does not incorporate business roles or is managed outside of the system manually

1. Creating a Business role
    a. When creating a business role we can define multiple types of roles into one single business role creating a single repository
    b. Creating business roles is very simple all we need to do is configure the connections of the applications we want to incorporate into a business role so that we have one source of the technical roles and they are contained in the business roles.
2. Maintaining a Business Role
    a. When managing the content of business roles rather than maintain multiple sources of information its all in one central location and we can easily update users access by just synchronizing the data in GRC or IAG to the end user.
    b. When we remove technical roles from a business role we can synchronize the business role to update all of the users affected and remove the technical role without having create new access requests or maintain the users manually
3. Inactivating a Business Role
    a. While the option is there to inactivate a business role but if it's no longer needed we can always inactivate so users are not able to request it.

Business Role integration points to other applications

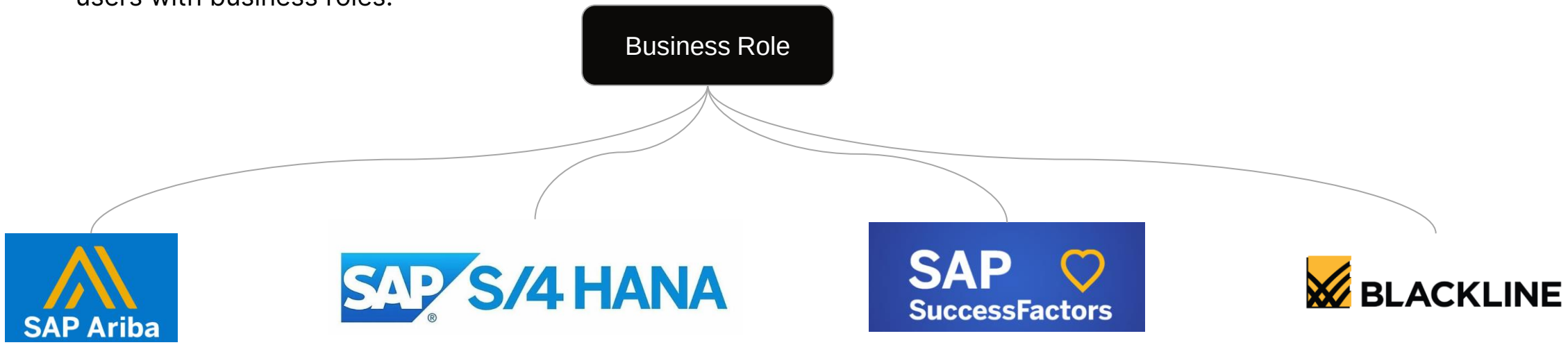
Customers that do not have a centralized business role concept are not able to integrate into risk analysis, access request management, and user access reviews. Along with being able to integrate business roles with other non-SAP applications.

1. Business Role Risk Analysis
    a. We can integrate Business Role development with workflow to execute risk analysis during the building of a business role.
    b. By Integrating Business Roles into Risk Analysis it facilitates the ability to see all of the existing risks that users would have.
    c. By consolidating into a business role model it provides additional role management and risk analysis reports to have real time information of existing users, roles, and risks.
2. Business Roles in Access Request Management and User Access Review
    a. There are many benefits to include Business Roles into the access request process with customers that use Business roles it improves the ability to find roles, it centralizes the access into a few business roles from many technical roles, and improves the efficiency of approvals in the access request process
    b. Integrating Business Roles in the User Access Review process improves the ability of role owners to be more effective
3. Integrating non-SAP Applications into Business Roles
    a. Many customers manage multiple applications and have not defined a centralized provisioning process. Business Roles can provide a solution to implement additional non-SAP roles into the Business Role model. This can be completed through integrating GRC 12 with IAG for SAP cloud solutions, GRC 12 with Pathlock, or integrating GRC 12 with SailPoint

Simplification of Business Role selection

Customers that do not have a business role concept have challenges with access request selection criteria during the request process or are not able to manage the role content effectively to reduce the time spent in identifying the necessary roles for users or the number of people required to determine what access is actually needed.

1. Business Roles can integrate the necessary applications into a single business role concept so that users only need to select a few business roles vs many technical roles that would be required to complete their job functions.
2. By simplifying the role content for all end users it improves the time it takes to complete access requests, it reduces the number of people required to provide input on role requirements for users and Consolidates the risk analysis of users with business roles.



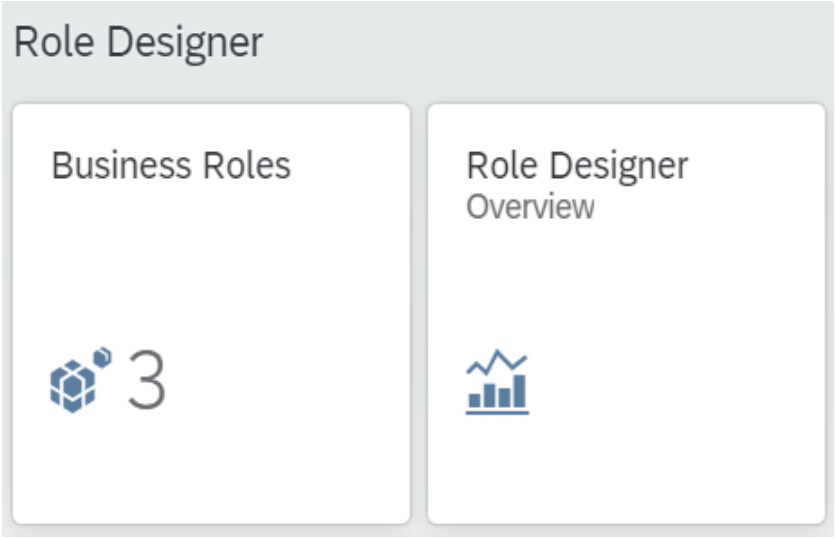
Business Role audit trail and reporting

Customers without a centralized business role concept are not able to quickly identify Business role content, business role usage, and business role audit requirements without having to go to multiple sources to gather the information.

1. Both GRC 12 and IAG provide reports for analyzing the data of business roles to users, actions in business roles, business role risk analysis
2. IAG has consolidated several reports into the role designer and Role Design Audit Log

GRC 12

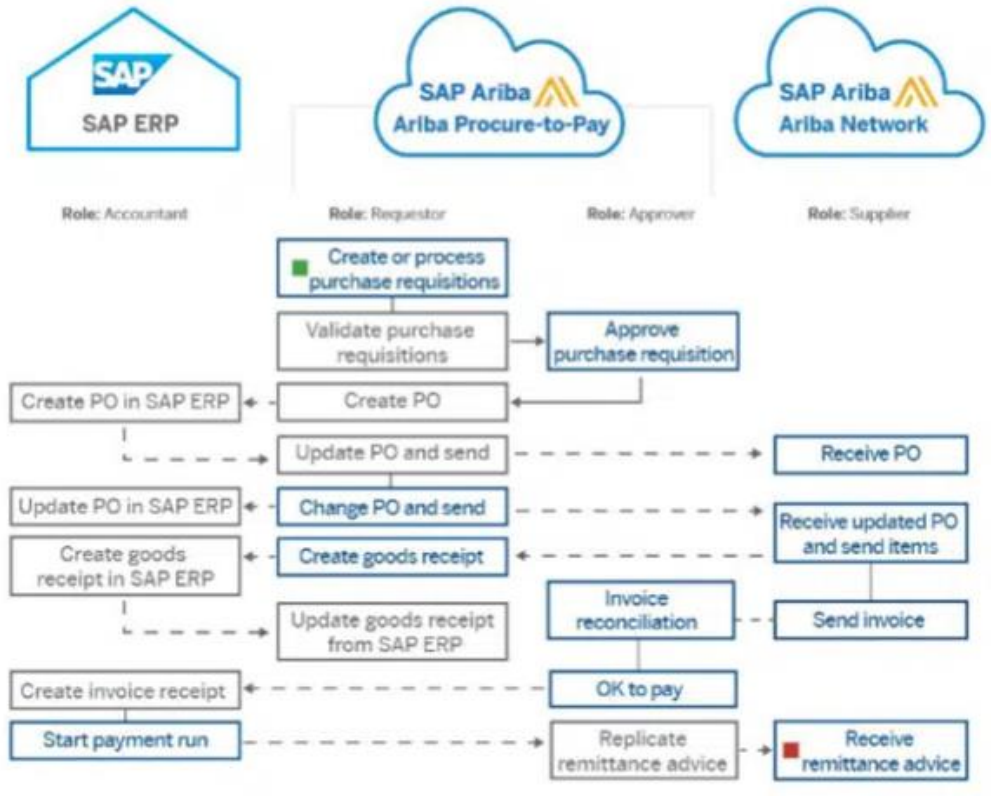
IAG



Managing Business Roles

Practical usage of business roles with existing processes

It is very important to understand the underlying processes and functional areas to be able to build the appropriate business roles.



Source: SAP

3. Business Role Management SAP GRC

Demo of Business Role Creation and Maintenance in GRC Access Control 12.0 and SAP Cloud Identity Access Governance

Demonstration

4. Business Role – the Good, the Bad, and the Ugly

The good, the bad, and the ugly of Business Roles, and explanation of how these can be successfully used in a realistic, compliant, self-service driven security while highlighting their challenges and potential issues they can cause as well.

Good vs Not So Good

As with every security concept and Maintenance application there are Pro's and Con's. Business Roles and Business Role Management are no exception to this.

Let's break down the Good, the Bad, and the Ugly for the "realistic usage" of Business Roles in a customer environment.

The “Good” of Business Roles

1. **Business Roles can be a mechanism to group a customers existing roles into larger and more “Meaningful” and “Business Friendly” End-User friendly design without needing to redesign your existing Single or Composite Roles behind the scenes.**

The benefits of this are:

- Ability to put the existing security puzzle pieces together that can be more End user focused using business language, a simplified business focused naming convention for the purposes of Access Requests, User Access Reviews and Role ownership while still leveraging your existing Security Roles masking the current complexity of your structure.

The “Good” of Business Roles

2. **Ability to build “Cross System Composite” Roles. (This is a big deal!)**

The benefits of this are:

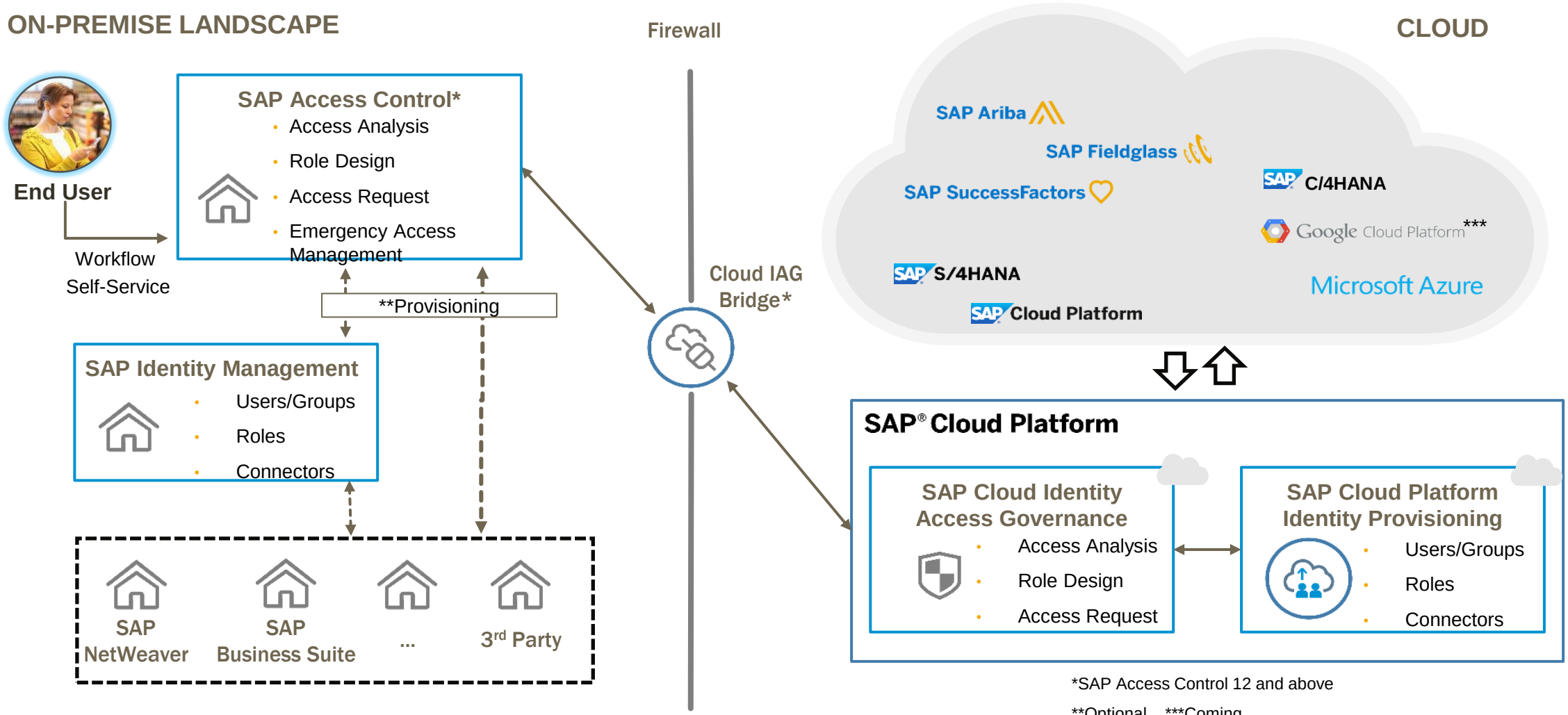
- This allows you to create roles that grant access across your entire system landscape for multiple systems all at once and keep them bundled together for easy selection and enforcement of “Access pre-requisites”.

- Many Security Admins are tasked with “needing to know” all role relationships and prerequisites otherwise end users risk not have the full access to perform their job.

  Example: “If you request the Purchas Order Admin Role you also need to have the standard Display role, a PO Approval role, the correct Fiori role, and the correct Active Director Group too otherwise the user will have access issues!”

Business Roles can allow you to bundle this together and have the system remember and enforce it rather than trying to teach the end-user, relying on a Security Admin, or a Role Mapping spreadsheet!

The “Good” of Business Roles – GRC and IAG Working Together for Cross Platform Capabilities



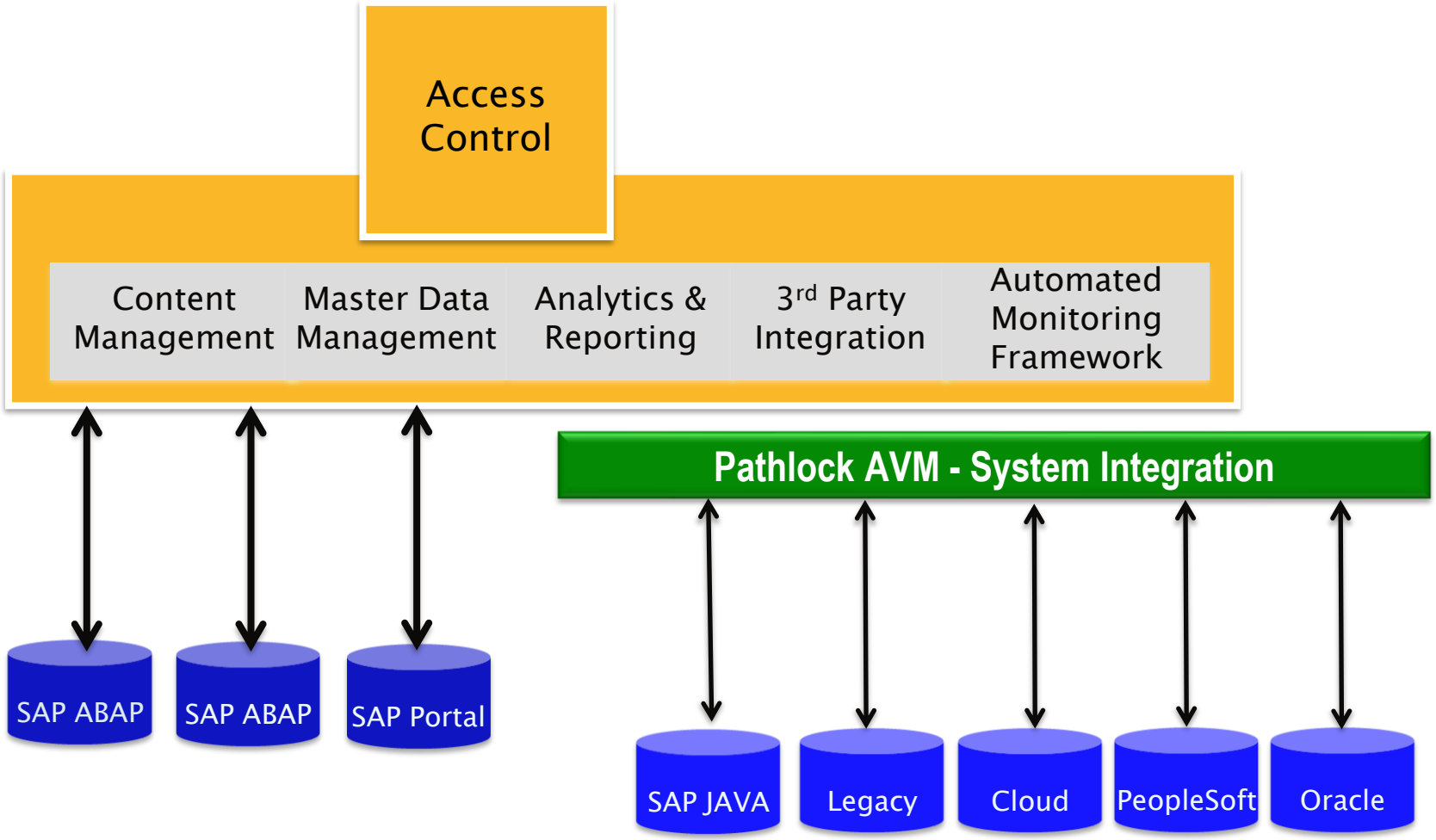
*SAP Access Control 12 and above

**Optional. ***Coming

Source: SAP

The “Good” of Business Roles – GRC and Pathlock Working Together for Cross Platform Capabilities

- Extend the capabilities of SAP Access Control across additional business applications and IT systems, eliminating administrative silos and enabling a more complete picture of user access across the organization.
- SAP Access Violation Management enables real-time risk analysis and provisioning, user access reviews, role management, and emergency access management to on-premise and cloud-based enterprise applications.



Source: Pathlock

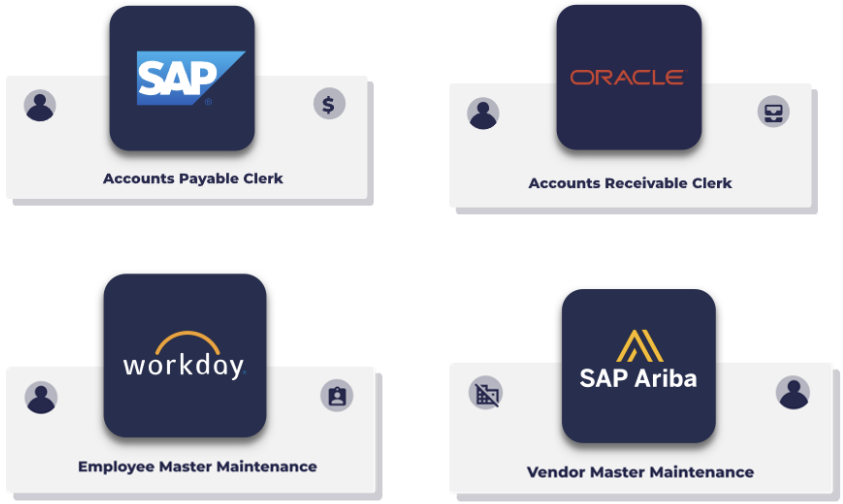
The “Good” of Business Roles – GRC and Pathlock Working Together for Cross Platform Capabilities

Uncover access risk & review user entitlements across applications

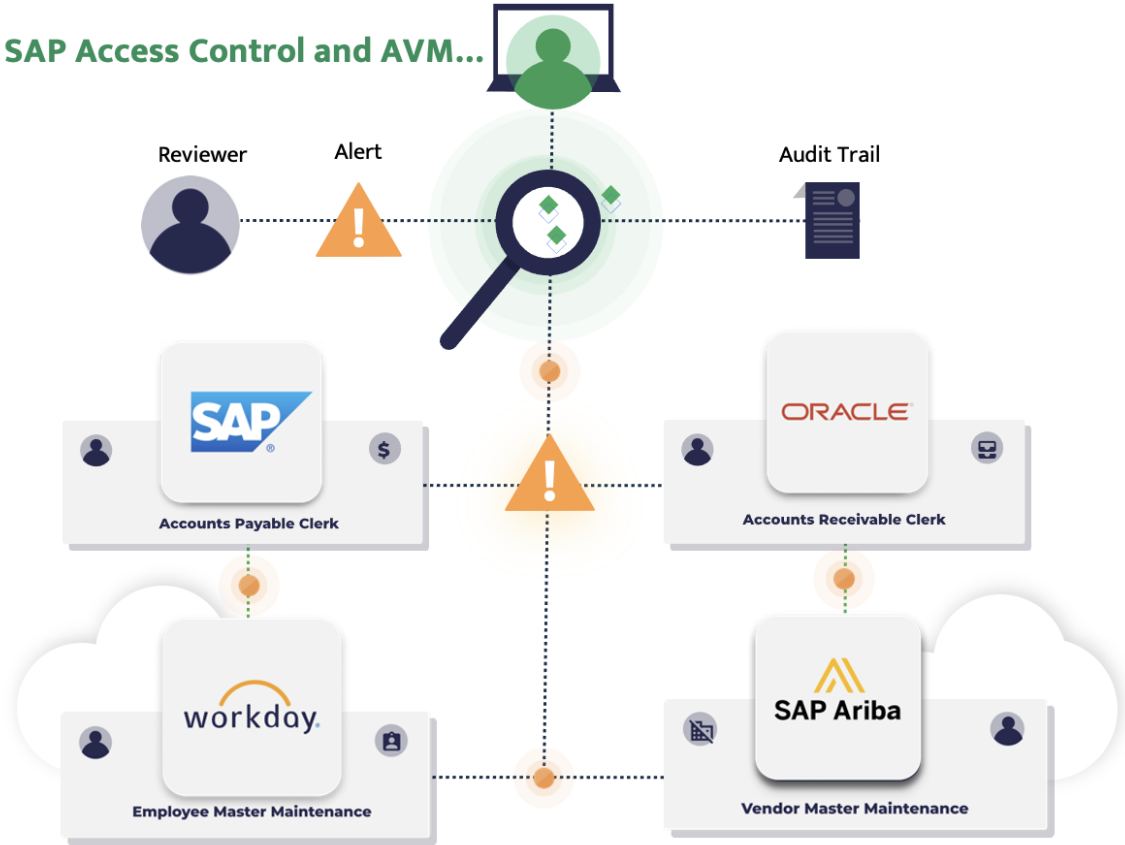
With a single pane of glass for identity and access governance

Current ...

- ❑ Access is managed and reviewed independently by system
- ❑ No cross-system access analysis
- ❑ Segregation of duties violation goes undetected



SAP Access Control and AVM...



Source: Pathlock

The “Good” of Business Roles

3. **Business Roles Provide the ability to Run Risk analysis and User Access Reviews at the higher and combined level rather then just at the individual Single and Composite role level.**

The benefits of this are:

- Having to Run SoD simulation on multiple Single and Composite roles together in GRC can be very time consuming. Business Roles provides a streamlined consolidation process in GRC that is used for SoD analysis, Provisioning, and User Access Review purposes.

- In UAR, Approvers are able to view and approve existing access at the higher structure level of the Business Role rather than having to deal with potentially hundreds of lines representing all the Single and Composite Roles a user may have assigned to them.

The “Good” of Business Roles

4. **Business Roles can serve as a potential alternative for “Reference User” functionality that many customers are utilizing today but wanting to replace so they can utilize todays new automated Workflow driven Provisioning and IDM applications.**

The benefits of this are:

- Although the SAP Security concept and functionality of Reference Users has been around for many years and technical operates well, it is unfortunately not supported by many Access Provisioning applications and Identity Management Systems.

- Business Roles can be an alternative to have similar Security access grouping functionality of Reference Users but also provide a supported platform that can integrate into modern IDM and Provisioning applications

The “Good” of Business Roles

5. **Business Roles are compatible with SAP GRC and IDM integrations and align with the Enterprise Busines Role concept that many Identity Management applications advocate.**

The benefits of this are:

- If you in the process of implementing an IDM system such as SailPoint, SAP IDM, or even SAP GRC for Access Requests and Provisioning capabilities, SAP Business Roles are supported by these applications. This allows you to leverage the benefits of simplifying Role selection and Access Permission bundling to these applications as well.

The “Bad and Ugly” of Business Roles

1. **The Business Role concept ONLY exists and is managed by SAP GRC Access Control and/or SAP Cloud IAG applications. They are NOT managed by the traditional SAP Security Transaction codes of PFCG or SU01/SU10 etc….**

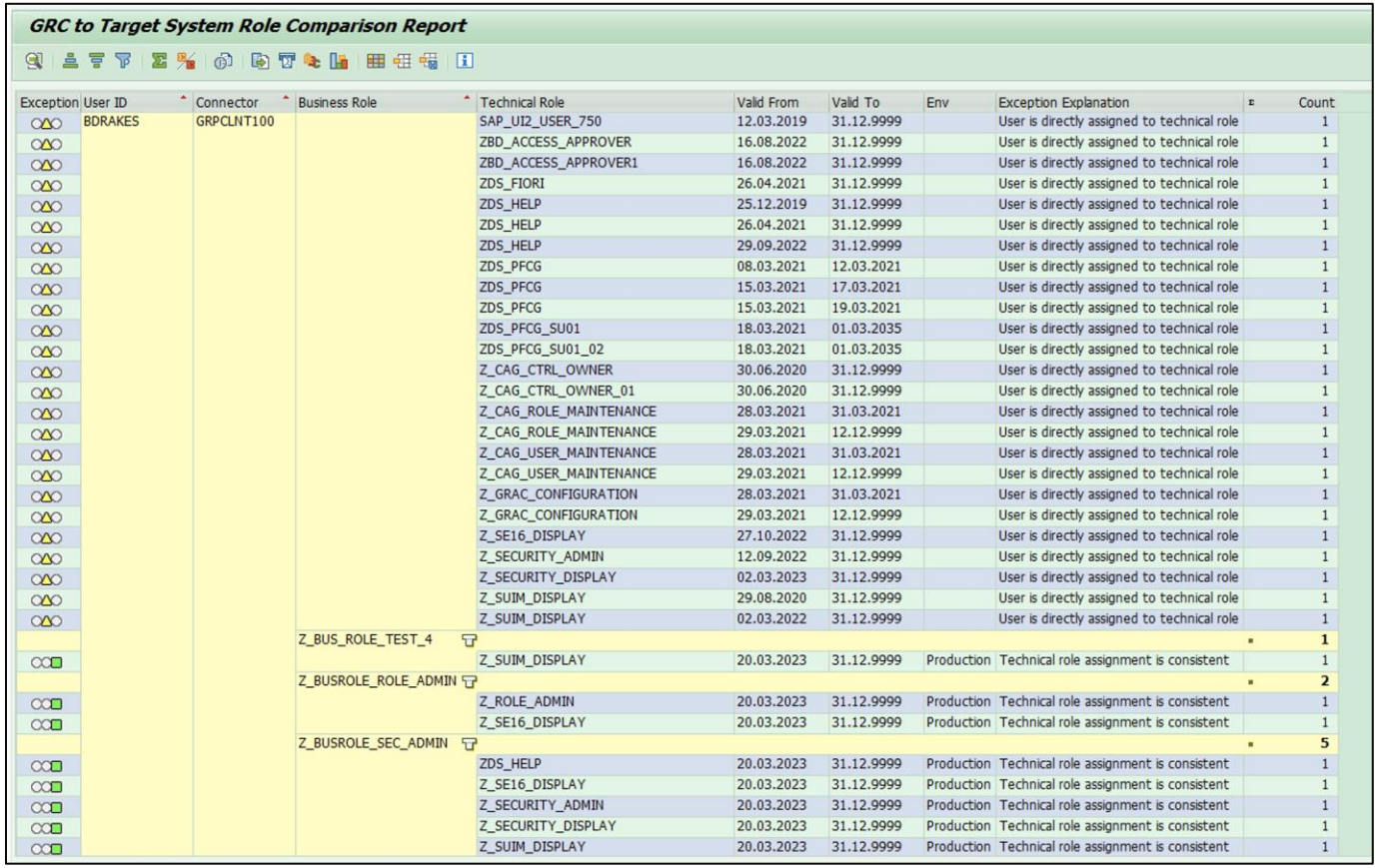
The Challenges are:

- Business Roles and their associated single and composite roles must ONLY be provisioned and maintained at the user level by the SAP GRC or SAP Cloud IAG applications. If you decide to remove access from a User via SU01, PFCG, SU10 things will get out of sync.
- This also means that if you are planning to implement SAP Business Roles, all end user access MUST be re-provisioned via an SAP GRC Access Request even if you are giving them the same access they had previously.
- SAP currently does not provide a Business Role migration or Re-assignment application.

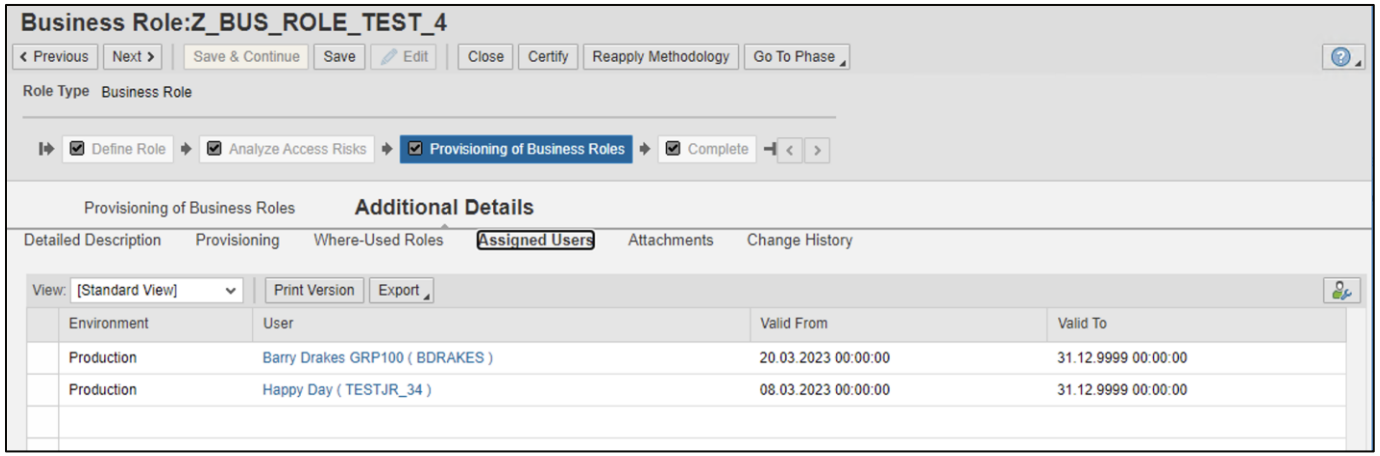
The “Bad and Ugly” of Business Roles

There is some good news for this challenge, Business Role synchronization issues can be identified via an SAP supplied report: **(GRAC_CHECK_BROLE_ASSIGNMENT)**

Also you can re-synchronize the role assignments to correct discrepancies for all users who possess the Business role on mass in BRM via the Provisioning stage in the SAP GRC Business Role Maintenance workflow.



Exception	User ID	Connector	Business Role	Technical Role	Valid From	Valid To	Env	Exception Explanation	Count
	BDRAKES	GRPCLNT100		SAP_UI2_USER_750	12.03.2019	31.12.9999		User is directly assigned to technical role	1
				ZBD_ACCESS_APPROVER	16.08.2022	31.12.9999		User is directly assigned to technical role	1
				ZBD_ACCESS_APPROVER1	16.08.2022	31.12.9999		User is directly assigned to technical role	1
				ZDS_FIORI	26.04.2021	31.12.9999		User is directly assigned to technical role	1
				ZDS_HELP	25.12.2019	31.12.9999		User is directly assigned to technical role	1
				ZDS_HELP	26.04.2021	31.12.9999		User is directly assigned to technical role	1
				ZDS_HELP	29.09.2022	31.12.9999		User is directly assigned to technical role	1
				ZDS_PFCG	08.03.2021	12.03.2021		User is directly assigned to technical role	1
				ZDS_PFCG	15.03.2021	17.03.2021		User is directly assigned to technical role	1
				ZDS_PFCG	15.03.2021	19.03.2021		User is directly assigned to technical role	1
				ZDS_PFCG_SU01	18.03.2021	01.03.2035		User is directly assigned to technical role	1
				ZDS_PFCG_SU01_02	18.03.2021	01.03.2035		User is directly assigned to technical role	1
				Z_CAG_CTRL_OWNER	30.06.2020	31.12.9999		User is directly assigned to technical role	1
				Z_CAG_CTRL_OWNER_01	30.06.2020	31.12.9999		User is directly assigned to technical role	1
				Z_CAG_ROLE_MAINTENANCE	28.03.2021	31.03.2021		User is directly assigned to technical role	1
				Z_CAG_ROLE_MAINTENANCE	29.03.2021	12.12.9999		User is directly assigned to technical role	1
				Z_CAG_USER_MAINTENANCE	28.03.2021	31.03.2021		User is directly assigned to technical role	1
				Z_CAG_USER_MAINTENANCE	29.03.2021	12.12.9999		User is directly assigned to technical role	1
				Z_GRAC_CONFIGURATION	28.03.2021	31.03.2021		User is directly assigned to technical role	1
				Z_GRAC_CONFIGURATION	29.03.2021	12.12.9999		User is directly assigned to technical role	1
				Z_SE16_DISPLAY	27.10.2022	31.12.9999		User is directly assigned to technical role	1
				Z_SECURITY_ADMIN	12.09.2022	31.12.9999		User is directly assigned to technical role	1
				Z_SECURITY_DISPLAY	02.03.2023	31.12.9999		User is directly assigned to technical role	1
				Z_SUIM_DISPLAY	29.08.2020	31.12.9999		User is directly assigned to technical role	1
				Z_SUIM_DISPLAY	02.03.2022	31.12.9999		User is directly assigned to technical role	1
			Z_BUS_ROLE_TEST_4						1
				Z_SUIM_DISPLAY	20.03.2023	31.12.9999	Production	Technical role assignment is consistent	1
			Z_BUSROLE_ROLE_ADMIN						2
				Z_ROLE_ADMIN	20.03.2023	31.12.9999	Production	Technical role assignment is consistent	1
				Z_SE16_DISPLAY	20.03.2023	31.12.9999	Production	Technical role assignment is consistent	1
			Z_BUSROLE_SEC_ADMIN						5
				ZDS_HELP	20.03.2023	31.12.9999	Production	Technical role assignment is consistent	1
				Z_SE16_DISPLAY	20.03.2023	31.12.9999	Production	Technical role assignment is consistent	1
				Z_SECURITY_ADMIN	20.03.2023	31.12.9999	Production	Technical role assignment is consistent	1
				Z_SECURITY_DISPLAY	20.03.2023	31.12.9999	Production	Technical role assignment is consistent	1
				Z_SUIM_DISPLAY	20.03.2023	31.12.9999	Production	Technical role assignment is consistent	1



The “Bad and Ugly” of Business Roles

2. **Business Role configuration and content details only reside in the SAP GRC systems. As a result, they are not Transportable Objects like Single, Derived, and Composite Roles.**

The Challenges are:

- A different change control process needs to be established using SAP GRC Business Role Management to enforce proper change control, approvals, and version management.

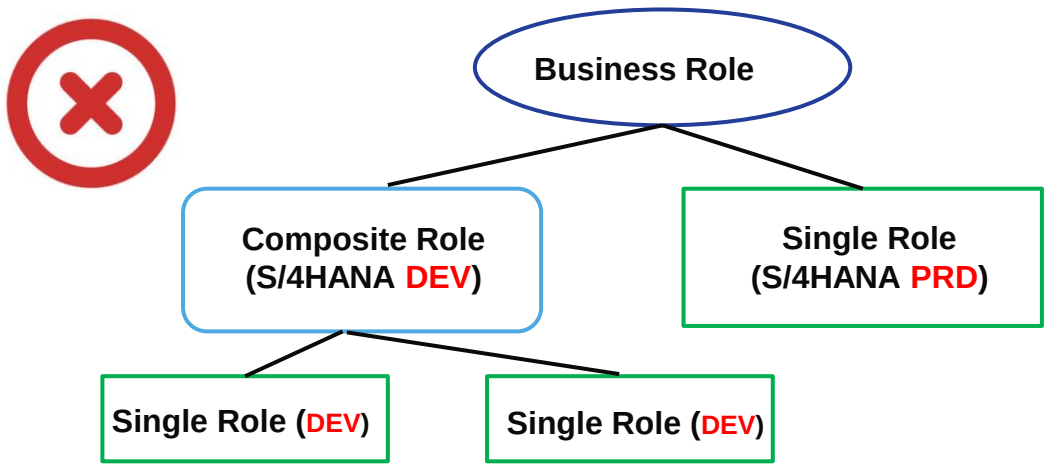
- In addition, Business Role change history and audit trail information resides in the SAP GRC and/or SAP Cloud IAG system rather than the traditional SAP Security change reporting areas familiar to SAP Security Administrators.

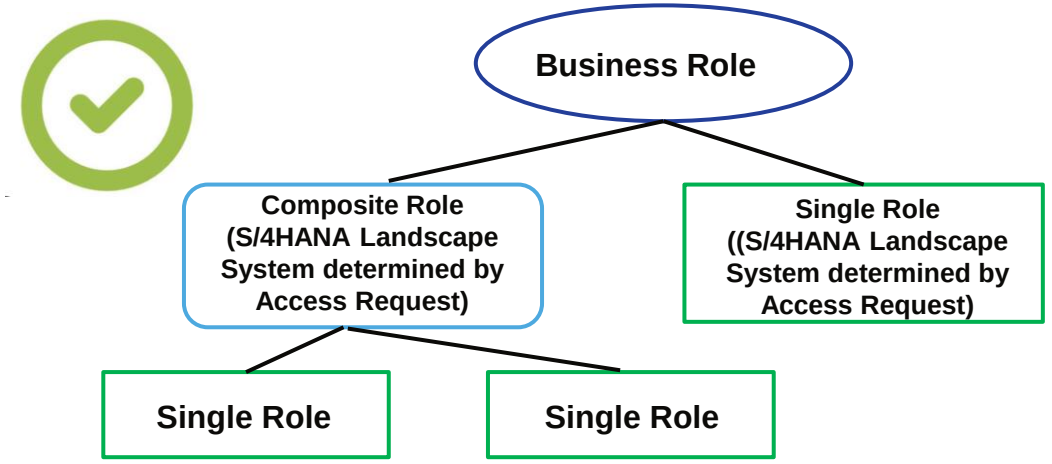
The “Bad and Ugly” of Business Roles

3. **Business Roles do not have the ability to isolate access between multiple systems in the same “landscape” such as Prod and Non-Prod. To separate out PRD vs Non-PRD assignments in the same Landscape, this must be selected and managed via Access Request Management Process.**

The Challenges are:

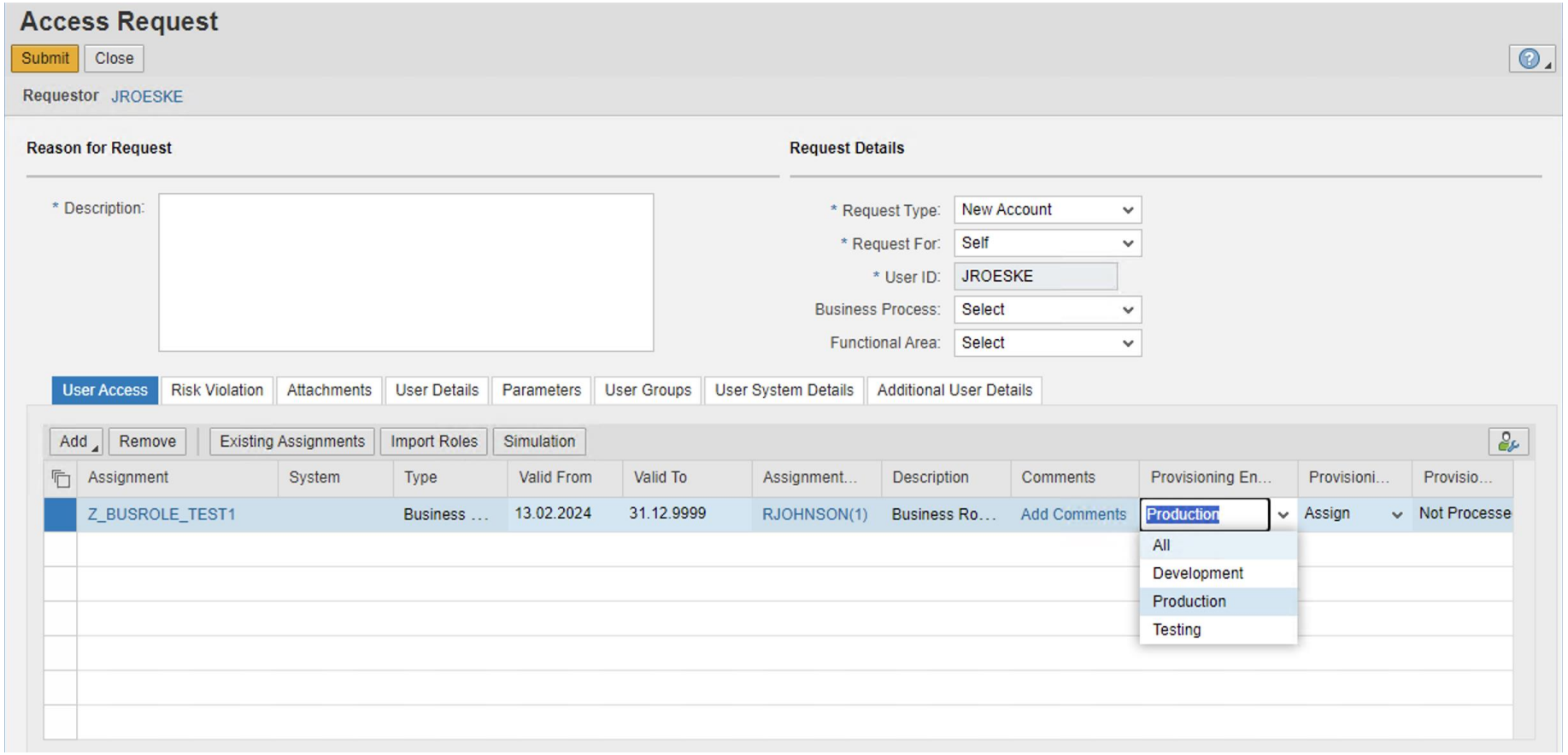
- This means that although Business Roles are “Cross System Composites”, you do not have the ability to specify a mixture of Production and Non-production system access into a single Business Role.





The “Bad and Ugly” of Business Roles

The SAP Access Request provides the mechanism to choose the “Provisioning Environment” the access should be provisioned to. As a result, you are not able to mix different systems in the same Landscape in the Business Role configuration.



The “Bad and Ugly” of Business Roles

4. **Business Roles have their own Owner assignments in SAP GRC, and do not leverage or inherit the Owners of the Single or Composites roles they may contain.**

The Challenges are:

- Many customers who leverage Business Roles bundle Single and Composite roles that potentially cross traditional Business functions and Ownership areas. This requires them to also consolidate Accountability and Ownerships for approval purposes to identify a single Owner that now spans multiple Business Functions or systems.

The “Bad and Ugly” of Business Roles

5. **The potential for Business Role structure complexity.**
   (Just because you can so do something, doesn’t mean you should!)

The Challenges are:

- When designing Busines Roles you have the technical capability to add Single, Composite, and even other Business Roles together into as many Business Roles as you like. There is no specific technical limit. Therefore, your Business Role design can become very complex quickly, resulting in additional troubleshooting to find out where access is specifically coming from for an End-user if you do not have a clear, structured, and detailed design.

- This is similar to the complexity that all Security Administrators face with Composite roles, but now it is expanded across multiple systems and platforms due to the extended capability that Business Roles bring to the table.

5. Business Role Management Implementation Approach

Cover implementation approach, effort, and steps to properly implement the Business Role concept into an existing customer environment.

Business Role Roadmap

How to implement Business roles based on your existing environment

there are various phases of implementing Business Roles it all depends on where you are with your existing SAP system or if its a brand-new SAP GRC or IAG implementation.

Phase 1	Phase 2	Phase 3	Phase 4
• No GRC system has been implemented • Only using standard SAP roles • Risk Analysis is not part of the role development • Approvals are obtained outside of a centralized system	• Existing SAP environment but very little GRC functionality has been implemented • Role content is managed through spreadsheets or in multiple sources • Technical roles have not been redesigned for a simpler approach • Business Roles have not been implemented	• GRC functionally is in place with the exception of business roles • Technical roles have been redesigned • Managing of user and role is challenging • Need to incorporate business roles into the existing environment • Not all workflows are in place	• GRC functionality is in place including • Technical roles have been redesigned • additional non SAP applications have been incorporated into the WF approval process for access requests • Role management reports are monitored and only need to add business roles

Business Role Implementation Steps

Where to start if you want to implement a streamlined Business Role concept into a GRC or IAG environment.

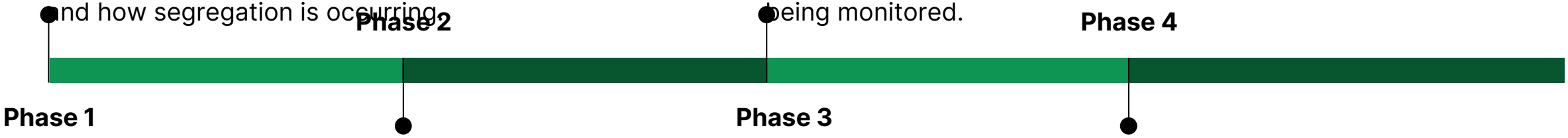
There are multiple steps required to have a fully functioning Business Role Environment. We will cover the major tasks that should be completed

Assess the current environment

Review the existing SAP Security design in place. Understand who has what access, what roles tcodes are in, and how segregation is occurring.

Build the new role design concept

Build the new technical roles, map technical roles into business roles, map existing users into technical roles and update the necessary rules with any access not being monitored.



Design a new role concept

Design what the new role concept will be, how access will be segregated, how it will be provisioned and who are the owners of the new role concept.

Deploy the new role concept

When deploying business roles to users it is necessary to request the new Business roles through an access request for all of the business role integration concepts to work effectively.

Business Role Concepts for Existing Environments

Customers already have GRC in place and only need to implement business roles

If you have an existing SAP GRC or IAG environment how should a business role implementation be approached.

Phase 1	Phase 2	Phase 3	Phase 4
• No GRC system has been implemented • Only using standard SAP roles • Risk Analysis is not part of the role development • Approvals are obtained outside of a centralized system	• Existing SAP environment but very little GRC functionality has been implemented • Role content is managed through spreadsheets or in multiple sources • Technical roles have not been redesigned for a simpler approach • Business Roles have not been implemented	• GRC functionally is in place with the exception of business roles • Technical roles have been redesigned • Managing of user and role is challenging • Need to incorporate business roles into the existing environment • Not all workflows are in place	• GRC functionality is in place including • Technical roles have been redesigned • additional non SAP applications have been incorporated into the WF approval process for access requests • Role management reports are monitored and only need to add business roles

Business Role Concepts for New Environments

If you have a new SAP GRC or IAG environment how should a business role implementation be approached.

Phase 1	Phase 2	Phase 3	Phase 4
• No GRC system has been implemented • Only using standard SAP roles • Risk Analysis is not part of the role development • Approvals are obtained outside of a centralized system	• Existing SAP environment but very little GRC functionality has been implemented • Role content is managed through spreadsheets or in multiple sources • Technical roles have not been redesigned for a simpler approach • Business Roles have not been implemented	• GRC functionally is in place with the exception of business roles • Technical roles have been redesigned • Managing of user and role is challenging • Need to incorporate business roles into the existing environment • Not all workflows are in place	• GRC functionality is in place including • Technical roles have been redesigned • additional non SAP applications have been incorporated into the WF approval process for access requests • Role management reports are monitored and only need to add business roles

Business Role Implementation pitfalls

What are the items to consider when planning on moving to Business Roles.

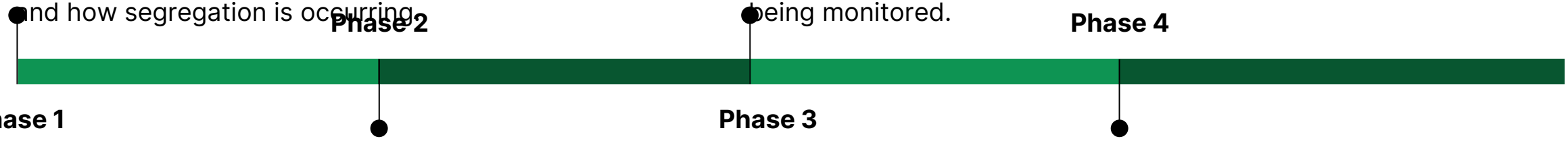
1. What is the existing Security design
2. How to start reviewing the SAP Access requirements
3. Who should be involved in those discussions
4. How do we plan to transition to business roles
5. Once in business roles what are the best practices to support it

Assess the current environment

Review the existing SAP Security design in place. Understand who has what access, what roles tcodes are in, and how segregation is occurring.

Build the new role design concept

Build the new technical roles, map technical roles into business roles, map existing users into technical roles and update the necessary rules with any access not being monitored.



It all starts with Planning

Design a new role concept

Design what the new role concept will be, how access will be segregated, how it will be provisioned and who are the owners of the new role concept.

Deploy the new role concept

When deploying business roles to users it is necessary to request the new Business roles through an access request for all of the business role integration concepts to work effectively.

Wrap Up

Questions and Further Discussion?

Where to Find More Information

https://help.sap.com/docs/SAP_CLOUD_IDENTITY_ACCESS_GOVERNANCE?locale=en-US&task=implement_task

- SAP Cloud IAG Integration Scenario Documentation

https://me.sap.com/notes/3311687

- 3311687 - Central KBA for GRC Business Role Management - How-to scenario, standard behavior or Guides

https://me.sap.com/notes/2072149

- 2072149 - Concept of Business Roles - Details & Inconsistency Check

https://me.sap.com/notes/3258752

- 3258752 - SAP Cloud IAG - How To's and Guides

https://me.sap.com/notes/2750594

- 2750594 - IAG - Create Candidate Business Role

https://me.sap.com/notes/2068247

- 2068247 - Delivered Adapters with SAP Regulation Management by Pathlock and SAP Access Violation Management by Pathlock

Key Points to Take Home

- Business Roles, although a relatively new Security feature brought in by SAP GRC, can be a very integral and beneficial addition to a customers existing Security design to organize, simplify, and consolidate End User access.
- As with every security concept and Maintenance application there are Pro's and Con's and SAP Business Role concept is not exception. Understanding the strengths and weaknesses of the Business Roles and BRM Functionality is essential for a successful implementation.
- GRC integration will facilitate the compliance checks needed to maintain a Business Role environment with SoD checks and audit trails of changes and Business Role Provisioning.
- Identify in which step of the "Business Role roadmap" you are currently in to successfully plan to implement Business Roles in your existing environment or future deployments.
- Once Business Roles are built it is important to plan the transition of users from technical roles to Business Roles. So always make sure that a plan is in place to perform the Business Role assignments

Thank you! Any Questions?

James E. Roeske • Chief Executive Officer
Customer Advisory Group • Think Big - Start Small - Work Smart with CAG
m. +1-403-606-0987 | t. +1-888-477-4950
e. James.Roeske@CustomerAdvisoryGroup.com | w. http://www.CustomerAdvisoryGroup.com

Gabriel Perez . Senior GRC Customer Advisor - Process Control Practice Lead
Customer Advisory Group • Think Big - Start Small - Work Smart with CAG
m. +1-480-773-5762 | t. +1-888-477-4950
e. Gabriel.Perez@CustomerAdvisoryGroup.com | w. http://www.CustomerAdvisoryGroup.com

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 with more than 800,000 members worldwide.