Security Guide
Document version: 1.40 – 2015-10-26

CUSTOMER

SAP Access Control™ 10.1 / Process Control™ 10.1 / Risk Management™ 10.1

Document History

Caution

Before you start the implementation, make sure you have the latest version of this document. You can find the latest version at: help.sap.com/grc.

The following table provides an overview of the most important document changes.

Table 1

Version	Date	Description
1.00	2013-06-04	Release to customers.
1.10	2013-09-13	Communication Destinations section updated.
1.20	2013-11-15	Included references to SAP Fiori
1.30	2015-07-24	Updated for SPS 10. Added section *8.5 Values for GRAC_ACTRD Field*.
1.40	2015-10-26	Added `SAP_GRC_NWBC` role for PC and RM

Content

1 Introduction

SAP Access Control is an enterprise software application that enables organizations to control access and prevent fraud across the enterprise, while minimizing the time and cost of compliance. The application streamlines compliance processes, including access risk analysis and remediation, business role management, access request management, emergency access maintenance, and periodic compliance certifications. It delivers immediate visibility of the current risk situation with real-time data.

SAP Process Control is an enterprise software solution for compliance and policy management. The compliance management capabilities enable organizations to manage and monitor its internal control environment. This provides the ability to proactively remediate any identified issues, and then certify and report on the overall state of the corresponding compliance activities. The policy management capabilities support the management of the overall policy lifecycle, including the distribution and attestation of policies by target groups. These combined capabilities help reduce the cost of compliance and improve management transparency and confidence in overall compliance management processes.

SAP Risk Management enables organizations to balance business opportunities with financial, legal, and operational risks to minimize the market penalties from high-impact events. The application allows customers to collaboratively identify these risks and monitor them on a continuous basis. Stakeholders and owners are provided with such tools as analytic dashboards for greater visibility in mitigating risks in their areas of responsibility.

The access control, process control, and risk management applications use the same security components, therefore, the information in this guide is relevant to you if you implement only SAP Access Control, only SAP Process Control, only SAP Risk Management, or all applications. The security guide provides an overview of the application relevant security information. You can use the information in this document to understand and implement system security, and to understand and implement the application security features.

i Note

Unless explicitly stated, it is understood the information in this guide applies to **all three** applications.

i Note

For information about the changes to security from SAP Access Control 5.3 to SAP Access Control 10.1, see the *SAP Access Control 10.1 Migration Guide*.

⚠ Caution

This guide does not replace the daily operations handbook that we recommend customers create for their specific productive operations.

Target Audience

The security guide is written for the following audience, and requires existing knowledge of SAP security model and of PFCG, SU01, and Customizing tools:

- Technology consultants
- System administrators

About this Document

This Security Guide covers two main security areas:

Network and system security

This area covers the system security issues and addresses them in the following sections:

- Technical System Landscape
- Network and Communication Security
  - Communication Channel Security
  - Communication Destinations
  - Integration with Single Sign-on (SSO) Environments
  - Data Storage Security
  - User Administration
  - Trace and Log Files

Application Security

Application security is divided in to the following sections:

- Application Security for SAP Process Control and SAP Risk Management

  This section covers the application security information for the process control and risk management applications.
- Application Security for SAP Access Control

  This section covers the application security information for the access control application.

> Note
>
> For ease of reading, the application names may be abbreviated as follows:
>
> - AC is SAP Access Control
> - PC is SAP Process Control
> - RM is SAP Risk Management

2 Before You Start

Access Control, Process Control, and Risk Management use SAP NetWeaver, SAP NetWeaver Portal, and SAP NetWeaver Business Warehouse. Therefore, the corresponding security guides and other documentation also apply.

Table 2

Guide	Location
SAP NetWeaver ABAP Security Guide	service.sap.com/securityguide
SAP NetWeaver Business Warehouse Security Guide	

Important SAP Notes

These SAP Notes contain the most recent information about the applications, as well as corrections to the documentation.

Make sure that you have the up-to-date version of each SAP Note, available at help.sap.com/grc.

For a complete list of important SAP Notes for the applications, see the following:

- For Access Control, see the *SAP Access Control 10.1 Master Guide* at help.sap.com/grc-ac *Installation and Migration*.
- For Process Control, see the *SAP Process Control 10.1 Master Guide* at help.sap.com/pc *Installation and Migration*.
- For Risk Management, see the *SAP Risk Management 10.1 Master Guide* at help.sap.com/rm *Installation and Migration*.

Additional Information

For more information about specific topics, see the links as shown in the table below.

Table 3

Content	Quick Link on the SAP Service Marketplace
Security	service.sap.com/security
Security Guides	service.sap.com/securityguide
Related SAP Notes	service.sap.com/notes
Released platforms	service.sap.com/platforms
Network security	service.sap.com/network service.sap.com/securityguide
Technical infrastructure	service.sap.com/ti
SAP Solution Manager	service.sap.com/solutionmanager

➡ Recommendation

For more information about SAP Fiori, see SAP Access Control 10.1 documentation at help.sap.com/grc-ac.

3 Technical System Landscape

For information about the technical system landscapes, see the following *Master Guides*:

- For Access Control, see the *SAP Access Control 10.1 Master Guide* at help.sap.com/grc-ac *Installation and Migration*.
- For Process Control, see the *SAP Process Control 10.1 Master Guide* at help.sap.com/pc *Installation and Migration*.
- For Risk Management, see the *SAP Risk Management 10.1 Master Guide* at help.sap.com/rm *Installation and Migration*.

4 Network and Communication Security

The network topology for SAP Access Control, SAP Process Control, and SAP Risk Management is based on the topology used by the SAP NetWeaver platform. Therefore, the security guidelines and recommendations described in the SAP NetWeaver Security Guide also apply to the applications. You can use the information in this section to understand and implement the network and communication security for the process control and risk management applications.

For more information, see the following sections in the SAP NetWeaver Security Guide in the SAP Library:

- Network and Communication Security
- Security Aspects for Connectivity and Interoperability

4.1 Communication Channel Security

The following table contains the communication paths used by the access control, process control, and risk management applications, the connection protocol, and the transferred data type:

Table 4

Communication Path	Protocol	Type of Data Transferred	Data Requiring Special Protection
SAP NetWeaver ABAP server using SAP GUI	DIAG	All application data	Logon data
SAP NetWeaver Portal	HTTP/HTTPS	All application data	Logon data
DS Extraction (application server to BI system)	RFC	All application data	Logon data
Application server to BI system	HTTP/HTTPS	All application data	Logon data
BI system to application server	HTTP/HTTPS	All application data	Logon data
BusinessObjects Enterprise Server	TCP/IP	All application data	Logon data
SAP NetWeaver Business Client	HTTP/HTTPS	All application data	Logon data

DIAG and RFC connections can be protected using Secure Network Communications (SNC). HTTPS connections are protected using the Secure Sockets Layer (SSL) protocol.

More Information

- *Transport Layer Security* in the SAP NetWeaver Security Guide

- *Using the Secure Sockets Layer Protocol with SAP NetWeaver Application Server ABAP* on the SAP Help Portal.

4.2 Trusted/Trusting RFC Relationships

You can set up trusted and trusting Remote Function Call (RFC) relationships between two SAP systems. This allows secure RFC connections between the systems without sending passwords for logging on. The logon user must have the corresponding authorization object `S_RFCACL` in the trusting system. This trusted relationship is not specific to GRC applications, and is a function of SAP NetWeaver.

More Information

Trusted/Trusting Relationships Between SAP Systems on the SAP Help Portal

help.sap.com/saphelp_nw04/helpdata/en/8b/0010519daef443ab06d38d7ade26f4/content.htm

4.3 Communication Destinations

This information applies to Access Control, Process Control, and Risk Management. The tables list the various types of Remote Function Calls (RFC) available. These are set-up using transaction code, `SM59`.

> ➡ Recommendation
>
> For more information about non-SAP applications, see solutions provided by SAP partners.

Access Control

The following table lists the communication destinations needed by Access Control to communicate with other SAP and non-SAP systems:

Table 5

Destination	Comments
Access Control to SAP ERP with GRC plug-ins installed	This connection is used to connect environments after they are configured. For more information about the authorizations needed for Access Control, see RFC Authorization Objects for Access Control [page 12]. • `GRCPINW` plug-in is used for non-HR functions • `GRCPIERP` plug-in is used for HR functions and if you have Process Control
Access Control to itself	This connection is used to configure Odata services.

Destination	Comments
	Recommendation For more information, see the *SAP Access Control, Process Control, Risk Management 10.1 Installation Guide* at help.sap.com/grc. Refer to the *Configuring the SAP NetWeaver Gateway* [external document] section.

Process Control

The table below lists the required connection destinations for Process Control to communicate with other SAP components:

Table 6

Destination	Comments
Process Control to SAP ERP with GRC plug-ins installed	GRC plug-ins: ● `GRCPINW` is used for Continuous Monitoring (required if you use the ABAP Report, Configurable and Programmed Subscenarios). ● `GRCPIERP` plug-in is used for HR functions
Process Control to SAP ERP **without** GRC plug-In installed	If the GRC plug-in is not installed, you can use SAP Query or BI Query data sources. The BI Query is available through Operational Data Provisioning (ODP). For ODP use, verify your NetWeaver system requirements are met.

Risk Management

The table below lists the connection destinations for Risk Management to communicate with other SAP components:

Table 7

Destination	Comments
Risk Management to SAP ERP **without** GRC plug-in installed	Risk Management can use SAP Query or BI Query data sources. The BI Query is available through Operational Data Provisioning (ODP). For ODP use, verify your NetWeaver system requirements are met.

4.3.1 RFC Authorization Objects for Access Control

The information in this section applies only to Access Control. The table lists the authorization objects and values you must add to the RFC user to allow Access Control to communicate with other SAP and non-SAP capabilities.

Table 8

Object	Description	Authorization Field	Value
S_RFC	Authorization check for RFC Access	ACTVT	16
	N/A	RFC_NAME	/GRCPI/*

Object	Description	Authorization Field	Value
			BAPT RFC1 SDIF SDIFRUNTIME SDTX SUSR SUUS SU_USER SYST SYSU
		RFC_TYPE	FUGR
S_TCODE	Authorization check at transaction start	TCD	SU01
S_TABU_DIS	Table maintenance	ACTVT	3
		DICBERCLS	&NC& SC SS ZV&G ZV&H ZV&N
S_TOOLS_EX	Tools Performance Monitor	AUTH	S_TOOLS_EX_A
S_GUI	Authorization for GUI activities	ACTVT	*
S_USER_AGR	Authorizations: role check	ACTVT	*
		ACT_GROUP	*
S_USER_AUT	User Master Maintenance: Authorizations	ACTVT	*
		AUTH	*
		OBJECT	*
S_USER_GRP	User Master Maintenance: User Group	ACTVT	*
		CLASS	*
S_USER_PRO	User Master Maintenance Authorization Profile	ACTVT	*
		PROFILE	*
S_USER_SAS	User Master Maintenance: System-Specific Assignments	ACTVT	01 06 22

Object	Description	Authorization Field	Value
		ACT_GROUP	*
		CLASS	*
		PROFILE	*
		SUBSYSTEM	*
S_USER_SYS	User Master Maintenance: System for Central User Maintenance	ACTVT	78
		SUBSYSTEM	*
S_USER_TCD	Authorizations: transactions in roles	TCD	*
S_USER_VAL	Authorizations: filed values in roles	AUTH_FIELD	*
		AUTH_VALUE	*
		OBJECT	*
S_DEVELOP	ABAP Workbench	ACTVT	*
		DEVCLASS	SUSO
		OBJNAME	/GRCPI/*
		OBJTYPE	FUGR
		P_GROUP	*
S_ADDRESS1	Central address management	ACTVT	01 02 03 06
		ADGRP	BC01
PLOG	Personnel planning	INFOTYP	1000 1001
		ISTAT	*
		OTYPE	*
		PLVAR	*
		PPFCODE	*
		SUBTYP	*
P_TCODE	HR: Transaction code	TCD	SU01

4.4 Integration with Single Sign-On Environments

The information in this section applies to Access Control, Process Control, and Risk Management.

Process Control and Risk Management:

- support the Single Sign-On (SSO) mechanisms provided by SAP NetWeaver Application Server ABAP.
- support the security guidelines for user management and authentication described in the SAP NetWeaver Application Server Security Guide.
- leverage the SAP NetWeaver ABAP Server and SAP NetWeaver Portal infrastructure.

Secure Network Communications (SNC)

For more information about SNC, see *Secure Network Communications (SNC)* in the *SAP NetWeaver Application Server Security Guide*.

SAP Logon Tickets

For more information about SAP Logon Tickets, see *SAP Logon Tickets* in the *SAP NetWeaver Application Server Security Guide*.

Client Certificates

For more information about X.509 Client Certificates, see *Using X.509 Client Certificates* on the SAP Help Portal (help.sap.com).

4.5 Data Storage Security

The information in this section applies to Access Control, Process Control, and Risk Management. .

Master data and transaction data is stored in the database of the SAP system on which the application is installed. Data storage occurs in Organizational Management, Case Management and in separate tables for this purpose.

In some applications, you can upload documents into the system. The default document management system (DMS) for storing data is the SAP Content Server and Knowledge Provider (KPro) infrastructure. Once uploaded, the documents can be accessed using a URL. The application security functions govern authorization for accessing the URL directly in the portal. To prevent unauthorized access to the document through copying and sending the URL, a URL is only valid for a given user and for a restricted amount of time (the default is two hours).

If you choose to implement a different document management system, the data storage security issues are deferred to that particular DMS.

4.6 User Administration

The application user administration uses the mechanisms provided by SAP NetWeaver, such as user types, tools, and the password concept.

User Types

You use **user types** to specify different security policies for different types of users. For example, your policy may specify that individual users who perform tasks interactively have to change their passwords on a regular basis, but not those users under which background processing jobs run.

The following user types are required for the process control and risk management applications:

- Dialog users:
  - Required for logging on to the SAP GUI and Web Dynpro
- Communication users:
  - Required for executing Automated Controls. (Process control application only)
  - Required for KRI value extractions. (Risk management application only)
  - Required for RFC connection to the BI system

    This is a user on the target system. Configure this user according to the security requirements of the target system.
  - Required for RTAs. (Process control application only)

    This is a user on the target system. Configure this user according to the security requirements of the target system.
  - A communication user (WF-BATCH) is required to run the workflow infrastructure.

User Administration Tools

The applications use SAP NetWeaver Application Server ABAP user and role maintenance. The following lists the tools available to manage users:

Table 9

Tool	Detailed Description
Transaction SU01	Use SU01 for ABAP user management: create and update users and assign authorizations.
Transaction PFCG (Profile Generator)	Use PFCG for ABAP role maintenance and creating authorization profiles.
Customizing	Use transaction SPRO to open Customizing. You can use Customizing to configure and maintain the application.
SAP NetWeaver Portal	This is the application front end. Most users can access the application through the portal.
SAP NetWeaver Business Client (NWBC)	This is the application front end. Most users can access the application through NWBC.

For more information, see Customizing for Governance, Risk, and Compliance and the respective applications: Access Control, Process Control, and Risk Management.

4.7 Trace and Log Files

For information about trace and log files, see the *SAP Access Control/Process Control/Risk Management 10.1 Operations Guide* at help.sap.com/grc.

4.8 Configuring NW VSI in the Landscape

Access Control, Process Control and Risk Management provide the ability to upload documents. We recommend you scan all documents for potential malicious code before you upload them. You can use the NetWeaver Virus Scan Interface (NW VSI) to scan the documents. For more information, see *SAP Virus Scan Interface* in the SAP NetWeaver Library.

5 Application Security: Process Control and Risk Management

A user's access to screens and menus on the front-end is determined by the following:

- The applications that are installed
- The role type
- The authorizations granted to the role type

Application Authorizations

The following table lists examples of screens on the front-end you see based on the **applications** installed on your system:

Table 10

Item	Application
▶ *My Home* ▸ *Work Inbox* ◀	All
▶ *My Home* ▸ *My Delegation* ▸ *Approver Delegation* ◀	SAP Access Control
▶ *Global Compliance Structure* ▸ *Indirect Entity-Level Controls* ◀	SAP Process Control
▶ *Assessments* ▸ *Proposed Risks and Risk Evaluations* ◀	SAP Risk Management

For more information about the information architecture for the screens and menus delivered by SAP, see the *Appendix*.

Customizing Front-end Screens and Menus

You can configure user-specific front-end screens and menus in the Customizing activities accessed from the `SPRO` transaction.

> ⚠ Caution
>
> SAP does not recommend you customize the information architecture because if SAP provides updates to the content, then such changes update only the standard SAP-delivered repository and Launchpads. The changes do not directly update any customized versions.

You carry out the configuration activities from the transaction `SPRO`, ▶ *SAP Reference IMG* ▸ *Governance, Risk, and Compliance* ▸ *General Settings* ▸ *Maintain Customer Specific Menus* ◀. Modify

Maintain Authorizations for Applications Links and *Configure LaunchPad for Menus* according to your user's needs..

Privacy Concerns

Notify your users as required by your company's privacy policy that user information such as first Name, last Name, E-mail address, roles, and other personal information is stored by the program `GRAC_REPOSITORY_OBJECT_SYNC`.

Maintaining Authorizations

Access Control uses object level authorizations. Authorizations are granted to users based on the authorizations of specific roles and the authorization objects assigned to those roles. To maintain the authorizations, you use `PFCG` and the information in this guide about the delivered roles and authorization objects.

SAP provides a set of sample roles for Access Control, which include recommended authorizations. You can create your own PFCG roles or copy the sample roles to your customer namespace. Then modify them as needed.

5.1 First-Level and Second-Level Authorizations

The information in this section applies to both Process Control and Risk Management.

This configuration flag determines the approach that is used to perform user-role assignments. The default authorization is First-Level Authorization. You can choose to enable Second-Level Authorization in the IMG. For more information, see *Configuring Second-Level Authorizations*.

First-Level Authorizations

When first-level authorization is active, the users assigned to the Business User role (`SAP_GRC_FN_BUSINESS_USER`) are the users available for any entity-user-role assignment. Once a user is assigned to an entity-user-role, the user assigned to the entity inherits the authorizations associated with the corresponding application role, as configured in `PFCG`.

Example

The figure illustrates that **all users** are included in the pool of potential users for the subprocess owner and control owner roles.

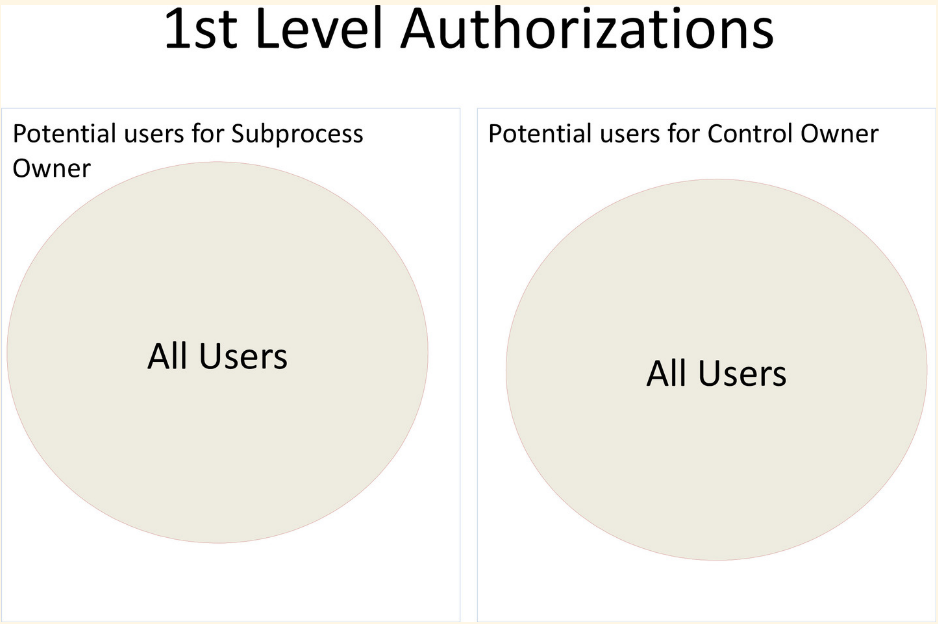

1st Level Authorizations
Potential users for Subprocess Owner
All Users
Potential users for Control Owner
All Users

Figure 1

First Level Authorization Details

Table 11

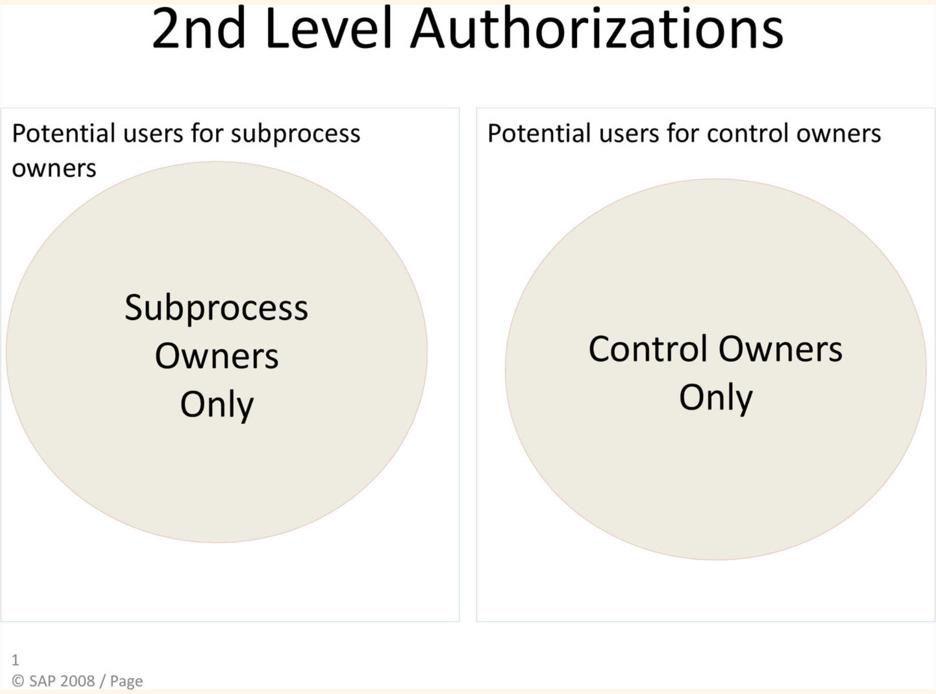
Authorizations	Entity Data Assignments	Delegation
• Business user role assignment • For all general users, this assignment is mandatory to access the application.	User assignment restricted to business users	Any business user can be a delegate and inherit data and authorizations.

Second Level Authorizations

In second-level authorization, the users available for an entity-user-role assignment are restricted to those users who have that specific application role assigned to their user profile. This allows the pool of business users to be segmented into different entity-user-role groups.

Example

The following figure illustrates that, in Process Control, you can define that only users assigned to the **Subprocess Owner** application role can be considered for **subprocess** entity-user-role assignments. Similarly, in Risk Management , you can define that only users assigned to the **Opportunity Owner** application role can be considered for **opportunity** entity-user-role assignments.



2nd Level Authorizations

Potential users for subprocess owners

Subprocess Owners Only

Potential users for control owners

Control Owners Only

1

© SAP 2008 / Page

Figure 2

Second-Level Authorization Details

Table 12

Authorizations	Entity Data Assignments	Delegation
• Business user role assignment	User assignment restricted to users assigned to application roles.	Any business user can be a delegate and inherit data and authorizations.

Authorizations	Entity Data Assignments	Delegation
• Application role assignment is required		

5.1.1 Configuring Second-Level Authorizations

You can enable and disable Second-Level Authorizations in the Customizing activity *Maintain Authorization Customizing* under *Governance, Risk, and Compliance* > *General Settings* > *Authorizations* > *Maintain Authorization Customizing*.

> Note
> - This setting is shared by both Process Control and Risk Management. Therefore, maintaining the setting for one application affects both applications.
> - This is a global setting and affects all application roles for your application.
> - Second-Level Authorizations affect only entity-user-role assignments while the feature is enabled. Entity-user-role assignments maintained prior to enabling Second-Level Authorizations may lose authorizations to perform certain activities in the application if they do not have the appropriate entity user-roles assigned. In this case, you must assign the additional authorizations to the specific users.

5.2 Delivered Roles

5.2.1 Process Control Application Roles

The information in this section applies only to Process Control. The delivered application roles are examples. You can copy them or create your own.

> Note
> SAP provides a BC Set for the role assignment customizing. If you choose to update the role assignment, do not assign the same role to multiple regulations.

Cross Regulation Roles

The following are the delivered application roles:

Table 13

Role	Role ID	Entity Level	Assigned by
Organization Admin	`SAP_GRC_SPC_GLOBAL_ORG_ADMIN`	Corporate	System Admin
Organization Owner	`SAP_GRC_SPC_GLOBAL_ORG_OWNER`	Organization	Organization Admin

Role	Role ID	Entity Level	Assigned by
Process and Control Admin	`SAP_GRC_SPC_GLOBAL_PRC_ADMIN`	Corporate	System Admin
Regulation and Policy Admin	`SAP_GRC_SPC_GLOBAL_REG_ADMIN`	Corporate	System Admin
Question and Survey Admin	`SAP_GRC_SPC_GLOBAL_SRV_ADMIN`	Corporate	System Admin
Test Plan Admin	`SAP_GRC_SPC_GLOBAL_TPL_ADMIN`	Corporate	System Admin
Automated Control Admin	`SAP_GRC_SPC_GLOBAL_AUT_ADMIN`	Corporate	System Admin
CEO/CFO	`SAP_GRC_SPC_GLOBAL_CEO_CFO`	Corporate	Organization Admin
Internal Auditor	`SAP_GRC_SPC_GLOBAL_INT_AUD`	Corporate	Organization Admin
Certification Admin	`SAP_GRC_SPC_SOX_SIG_ADMIN`	Corporate	Power User
CAPA Plan Approver	`SAP_GRC_SPC_FDA_CAPA_PLAN_APPR`	Corporate/Organization	Power User
CAPA Execution Approver	`SAP_GRC_SPC_FDA_CAPA_EXEC_APPR`	Corporate/Organization	Power User
Policy Admin	`SAP_GRC_SPC_CRS_PLC_ADMIN`	Corporate	System Admin
Policy Manager	`SAP_GRC_SPC_CRS_PLC_MANAGER`	Organization	System Admin
Policy Owner	`SAP_GRC_SPC_CRS_POLICY_OWNER`	Policy	Policy Admin
Policy Approver	`SAP_GRC_SPC_CRS_PLC_APPR`	Policy	Policy Admin
Policy Reviewer	`SAP_GRC_SPC_CRS_PLC_REVIEW`	Policy	Policy Admin
Policy Viewer	`SAP_GRC_SPC_CRS_PLC_DISPLAY`	Policy	Policy Admin
Ad Hoc Issue Admin	`SAP_GRC_SPC_CRS_ISSUE_ADMIN`	Corporate	System Admin
Ad Hoc Issue Processor	`SAP_GRC_FN_ADISSUE_PROCESS`	G_AI	System Admin

Role	Role ID	Entity Level	Assigned by
			Note You assign this role to users to allow them to process ad hoc issues. In the front-end, there is no need to assign this role to users via mass role assignment.
Continuous Monitoring Data Source Specialist	`SAP_GRC_SPC_CRS_CM_DS_SPEC`	Corporate	System Admin
Continuous Monitoring Business Rule Specialist	`SAP_GRC_SPC_CRS_CM_BR_SPEC`	Corporate	System Admin
Continuous Monitoring Job Specialist	`SAP_GRC_SPC_CRS_CM_JOB_SPEC`	Corporate	System Admin
Cross Regulation Internal Control Manager	`SAP_GRC_SPC_CRS_ICMAN`	Corporate	System Admin
Cross Regulation Organization Owner	`SAP_GRC_SPC_GLOBAL_ORG_OWNER`	Organization	Cross Regulation Internal Control Manger
Cross Regulation Organization Tester	`SAP_GRC_SPC_CRS_ORG_TESTER`	Organization	Cross Regulation Internal Control Manger
Cross Regulation Process Owner	`SAP_GRC_SPC_CRS_PRC_OWNER`	Process	Cross Regulation Internal Control Manger
Cross Regulation Subprocess Owner	`SAP_GRC_SPC_CRS_SPR_OWNER`	Subprocess	Cross Regulation Internal Control Manger
Cross Regulation Control Owner	`SAP_GRC_SPC_CRS_CTL_OWNER`	Control	Cross Regulation Internal Control Manger
Cross Regulation Control Tester	`SAP_GRC_SPC_CRS_PRC_TESTER`	Control	Cross Regulation Internal Control Manger

The delivered Cross Regulation roles have the following attributes:

- They are assigned the Portal role **GRC Suite**.
- They are assigned to the GRC work centers.
- They are assigned through the Access Management work center.
- They require the following standard roles:
  - `SAP_GRC_FN_BASE`
  - `SAP_GRC_FN_BUSINESS_USER`

> Note
>
> The role `SAP_GRC_FN_ADISSUE_PROCESS` grants the authority to process ad hoc issues. You do not need to assign this role to a user. The authorization is assigned through the application's code logic, and the user who is

assigned as the issue owner is automatically granted this authorization. You must ensure the role profile is activated.

SOX Regulation Application Roles

The following are the delivered application roles for the SOX regulation:

Table 14

Role	Role ID	Entity Level	Assigned by
SOX Internal Control Manager	SAP_GRC_SPC_SOX_ICMAN	Corporate	Regulation/Policy Admin
SOX Subprocess Owner	SAP_GRC_SPC_SOX_SPR_OWNER	Subprocess	SOX Internal Control Manager
SOX Control Owner	SAP_GRC_SPC_SOX_CTL_OWNER	Control	SOX Internal Control Manager
SOX Organization Owner	SAP_GRC_SPC_REG_ORG_OWNER_1	Organization	SOX Internal Control Manager
SOX Control Tester	SAP_GRC_SPC_SOX_PRC_TESTER	Control	SOX Internal Control Manager
SOX Organization Tester	SAP_GRC_SPC_SOX_ORG_TESTER	Organization	SOX Internal Control Manager
SOX Automated Rule Specialist	SAP_GRC_SPC_SOX_AUT_SPECIALIST	Corporate	SOX Internal Control Manager

The delivered SOX application roles have the following attributes:

- They are assigned by the SOX Internal Control Manager.
- They require the following standard roles:
  - SAP_GRC_FN_BASE
  - SAP_GRC_FN_BUSINESS_USER
  - They require the portal role: GRC Suite.

FDA Regulation Application Roles

The following are the delivered application roles for the FDA regulation:

Table 15

Role	Role ID	Entity Level	Assigned by
FDA Internal Control Manager	SAP_GRC_SPC_FDA_ICMAN	Corporate	Regulation/Policy Admin
FDA Subprocess Owner	SAP_GRC_SPC_FDA_SPR_OWNER	Subprocess	FDA Internal Control Manager
FDA Control Owner	SAP_GRC_SPC_FDA_CTL_OWNER	Control	FDA Internal Control Manager

Role	Role ID	Entity Level	Assigned by
FDA Control Tester	SAP_GRC_SPC_FDA_PRC_TESTER	Control	FDA Internal Control Manager
FDA Organization Owner	SAP_GRC_SPC_REG_ORG_OWNER_2	Organization	FDA Internal Control Manager
FDA Organization Tester	SAP_GRC_SPC_FDA_ORG_TESTER	Organization	FDA Internal Control Manager
FDA Automated Rule Specialist	SAP_GRC_SPC_FDA_AUT_SPECIALIST	Corporate	FDA Internal Control Manager

The delivered FDA application roles have the following attributes:

- They are assigned by the FDA Internal Control Manager.
- They require the following standard roles:
  - `SAP_GRC_FN_BASE`
  - `SAP_GRC_FN_BUSINESS_USER`
  - They require the portal role: GRC Suite

5.2.2 Risk Management Application Roles

The information in this section applies only to Risk Management. The delivered application roles are example roles. You can use them as is, copy them, or create your own.

Risk Management roles have the following attributes:

Table 16

Role	Role ID	Entity Level	Assigned by
Activity Owner	SAP_GRC_RM_API_ACTIVITY_OWNER	Activity, Corporate	Unit Risk Manager
Central Risk Manager	SAP_GRC_RM_API_CENTRAL_RM	Corporate, Organization	Power User
CEO/CFO	SAP_GRC_RM_API_CEO_CFO	Corporate, Organization	Central Risk Manager
Incident Editor	SAP_GRC_RM_API_INCIDENT_EDITOR	Incident	Unit Risk Manager
Internal Auditor	SAP_GRC_RM_API_INTERNAL_AUD	Corporate, Organization	Central Risk Manager
Opportunity Owner	SAP_GRC_RM_API_OPP_OWNER	Opportunity	Unit Risk Manager

Role	Role ID	Entity Level	Assigned by
Organization Owner	`SAP_GRC_RM_API_ORG_OWNER`	Corporate, Organization	Central Risk Manager
Risk Expert	`SAP_GRC_RM_API_RISK_EXPERT`	Risk	Unit Risk Manager
Risk Owner	`SAP_GRC_RM_API_RISK_OWNER`	Risk	Unit Risk Manager
System Administrator	`SAP_GRC_RM_API_LIAISON`	Corporate	Central Risk Manager
Unit Risk Manager	`SAP_GRC_RM_API_RISK_MANAGER`	Corporate, Organization	Central Risk Manager

- They are assigned through the User Access work set.
- They require the following standard roles:
  - `SAP_GRC_FN_BASE`
  - `SAP_GRC_FN_BUSINESS_USER`
- They require the portal role: GRC Risk Management.

5.2.3 Authorization Objects Contained in Application Roles

The application roles are composed of the following authorization objects:

- **GRFN_API**

  This is the most utilized authorization object. It controls access to the master data objects and drives the user authorizations for the business entities. It includes the following elements: activity, entity, subentity, and datapart.
- **GRFN_REP**

  This authorization object controls the access to retrieve data for reports. It has the elements: Activity and Report Name.
- **GRFN_CONN**

  This authorization object is used to run automated rules testing or monitoring on other systems. It grants **Remote Function Call** authority to the user. To assign this authorization to users, use transaction `SU01` in the back-end system to create a new role, add the authorization object to the role, and assign the role to users.

For more information about the possible element values, see *Authorization Object Elements* in the *Appendix*.

5.2.4 NWBC Roles

Process Control and Risk Management deliver the following NWBC role to allow users the authorization to launch NWBC and access menu items in NWBC. You must copy this role into your own namespace and assign it to all users who need to use NWBC.

Table 17

Role	Description
SAP_GRC_NWBC	Gives authorizations to launch NWBC. Assign this role to all NWBC users.

Note

Do not assign SAP_GRC_NWBC and SAP_GRAC_NWBC to the same user.

5.2.5 Portal Roles

This section provides information about the delivered portal roles for Process Control and Risk Management. The delivered portal roles are sample roles. You can use them as delivered, copy them, or create your own.

For information about the BOE portal roles, see the *BusinessObjects Enterprise XI 3.1 Publisher's Guide* and *BusinessObjects XI Integration for SAP Installation Guide* at help.sap.com/boe31 .

Process Control Portal Roles

Process Control has two delivered portal roles:

- GRC_Suite. This portal role must be assigned to all Process Control users.
- GRC Internal Audit Management. Assign this role to the user for Internal Audit Management processing. To use this role, the user must be also be assigned the GRC_Suite role and the user group must be assigned the ERP COMMON role.

Risk Management Portal Roles

Risk Management has one delivered portal role: COM.SAP.GRC.RM.Role_All (GRC Risk Management).

5.2.6 Continuous Monitoring Roles (Process Control)

The information in this section only applies to Process Control. This information covers the role authorizations required for Continuous Monitoring:

- Cross Regulation Data Source Specialist

  The user with this role can create and maintain the data sources. Assign the user the role SAP_GRC_FN_BUSINESS_USER using transaction SU01 in the Process Control back-end system.
- Cross Regulation Business Rule Specialist

The user with this role can create and maintain business rules. Assign the user the `SAP_GRC_FN_BUSINESS_USER` role in using transaction `SU01` in the Process Control back-end system.

- Cross Regulation Job Specialist

  The user with this role can create jobs in Monitoring Scheduler and monitor job status in Job Monitor. Assign the user the following roles in transaction `SU01` in the Process Control back-end system:

  ○ `SAP_GRC_FN_BUSINESS_USER`, which grants basic access to the application

  ○ `SAP_GRC_SPC_SCHEDULER`, which grants the authority to run background jobs

  To allow the user the authorization to execute SoD jobs, you must also assign the **SAP_GRAC_RISK_ANALYSIS** role, which grants the authority to run SoD jobs.

  > Note
  >
  > The role is delivered with Access Control, therefore, SoD jobs can only be run in the system where Access Control is also activated.

- Internal Control Manager/Process Owner/Subprocess Owner/Control Owner

  These users can access the Job Monitor and Event Queue Log to view the results. This role needs the PFCG standard role (`SAP_GRC_FN_BUSINESS_USER`) assigned.

- `Z_GRFN_CONN`

  This role is not delivered; you must create it. Assign the role to the connector for automated control testing and monitoring. Assign the role to users and application roles that require authorization to view the job results of automated control testing and monitoring. The user can only view results of information for the specific connector. The role uses the authorization object `GRFN_CONN`.

5.2.7 Internal Audit Management Roles (Process Control)

The information in this section applies only to Process Control. This information covers delivered roles standard for Internal Audit Management (IAM). The following table lists the authorization fields and values that are available for each authorization object in the delivered role:

Audit Director (SAP_GRC_IAM_AUD_DIR)

Table 18

Authorization Object	Field		Values	
Auditable Entity *(GRFN_AE)*	Activity	ACTVT	01	Create
	Activity	ACTVT	02	Change Note Cannot change *Name* or *Responsible Person.*
	Activity	ACTVT	03	Display
	Activity	ACTVT	06	Delete

Audit Risk Rating *(GRFN_ARR)*	Activity	ACTVT	01	Create, Copy
	Activity	ACTVT	02	Change Note Cannot change *Name* or *Responsible Person*.
	Activity	ACTVT	03	Display
	Activity	ACTVT	06	Delete
Audit Proposal *(GRFN_AP)*	Activity	ACTVT	01	Create
	Activity	ACTVT	02	Change Note Cannot change *Name* or *Responsible Person*.
	Activity	ACTVT	03	Display
	Activity	ACTVT	06	Delete
	Activity	ACTVT	50	Transfer
	Activity	ACTVT	64	Generate Note Requires authorization to generate audit plan proposal from audit risk rating.
Audit Plan Proposal*(GRFN_APP)*	Activity	ACTVT	01	Create
	Activity	ACTVT	02	Change Note Responsible person can change role; cannot change *Name* or *Responsible Person*.
	Activity	ACTVT	03	Display
	Activity	ACTVT	06	Delete
	Activity	ACTVT	50	Transfer

	Activity	ACTVT	64	Generate Note Requires authorization to generate audit proposal from audit risk rating.
IAM Reports *(GRFN_REP)*	Activity	ACTVT	71	Analyze
	Activity	ACTVT	80	Print
	Activity	ACTVT	*	All

Audit Manager (SAP_GRC_IAM_AUD_MGR)

Table 19

Authorization Object	Field		Values	
Auditable Entity *(GRFN_AE)*	Activity	ACTVT	01	Create
	Activity	ACTVT	02	Change Cannot change *Name* or *Responsible Person.*
	Activity	ACTVT	03	Display
	Activity	ACTVT	06	Delete
Audit Risk Rating *(GRFN_ARR)*	Activity	ACTVT	02	Change Note Responsible person can change or edit the audit risk rating. *Name* and *Responsible Person* cannot be changed.
	Activity	ACTVT	03	Display
Audit Proposal *(GRFN_AP)*	Activity	ACTVT	01	Create
	Activity	ACTVT	02	Change Cannot change *Name* or *Responsible Person.*
	Activity	ACTVT	03	Display
	Activity	ACTVT	06	Delete
	Activity	ACTVT	50	Transfer
	Activity	ACTVT	64	Generate

				Note Requires authorization to generate audit proposal from audit risk rating.
Audit Plan Proposal *(GRFN_APP)*	Activity	ACTVT	02	Change Note Responsible person cannot change role. Cannot change *Name* or *Responsible Person*.
	Activity	ACTVT	03	Display
	Activity	ACTVT	50	Transfer Note Only responsible person can transfer.
	Activity	ACTVT	64	Generate Note Requires authorization to generate audit plan proposal from audit risk rating.
Ad Hoc Issues *(GRFN_AUDIS)*	Activity	ACTVT	01	Create
IAM Reports *(GRFN_REP)*	Activity	ACTVT	71	Analyze
	Activity	ACTVT	80	Print
	Activity	ACTVT	*	All

Audit Lead (SAP_GRC_IAM_AUD_LEAD)

Table 20

Authorization Object	Field		Values	
Audit Risk Rating *(GRFN_ARR)*	Activity	ACTVT	03	Display
Audit Proposal *(GRFN_AP)*	Activity	ACTVT	02	Change

				Note Only responsible person can change or edit the audit plan.*Name* and *Responsible Person* cannot be changed.
	Activity	ACTVT	03	Display
Audit Plan Proposal *(GRFN_APP)*	Activity	ACTVT	03	Display
IAM Reports *(GRFN_REP)*	Activity	ACTVT	71	Analyze
	Activity	ACTVT	80	Print
	Activity	ACTVT	*	All

5.3 Workflow Recipient

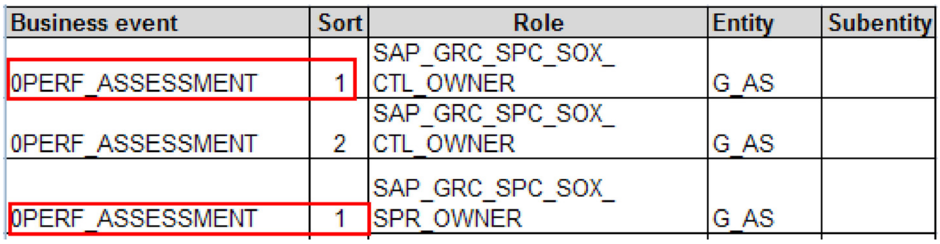
The applications determine the agent (or recipient) of a workflow task based on the mapping of business events and roles. You can override the default configuration and maintain your own agent determination rule in the Customizing activities (using the `SPRO` transaction). Carry out the activity *Maintain Custom Agent Determination Rules* under ▶ *Governance, Risk, and Compliance* ▶ *General Settings* ▶ *Workflow* ◀

In the *Customized Business Events* table, you configure rules for determining the recipient of a workflow task by customizing the business events, sort, roles, entities, and subentities.

5.3.1 Maintaining Workflow Recipient Rules

The following is an overview for maintaining the workflow recipient rules:

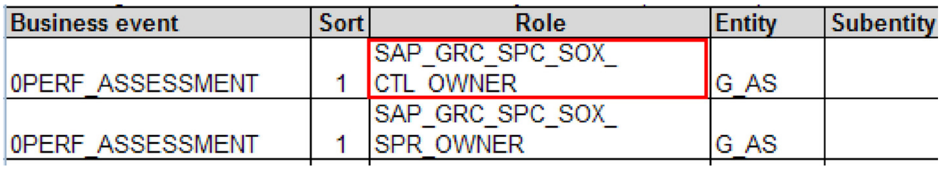
- The value of the sort number has no numerical significance. It is only for grouping. The following figure illustrates that the Perform Assessment business event for SOX Control Owner is in the same group as the SOX Subprocess Owner.



Business event	Sort	Role	Entity	Subentity
0PERF_ASSESSMENT	1	SAP_GRC_SPC_SOX_CTL_OWNER	G_AS	
0PERF_ASSESSMENT	2	SAP_GRC_SPC_SOX_CTL_OWNER	G_AS	
0PERF_ASSESSMENT	1	SAP_GRC_SPC_SOX_SPR_OWNER	G_AS	

Figure 3

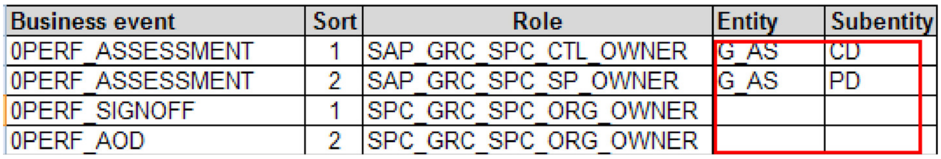
- The business event processing starts with the lowest entity-level role and proceeds upwards. In the following example, control owner is lower than subprocess owner in the entity-level hierarchy, therefore it is processed first.



Business event	Sort	Role	Entity	Subentity
0PERF_ASSESSMENT	1	SAP_GRC_SPC_SOX_CTL_OWNER	G_AS	
0PERF_ASSESSMENT	1	SAP_GRC_SPC_SOX_SPR_OWNER	G_AS	

Figure 4

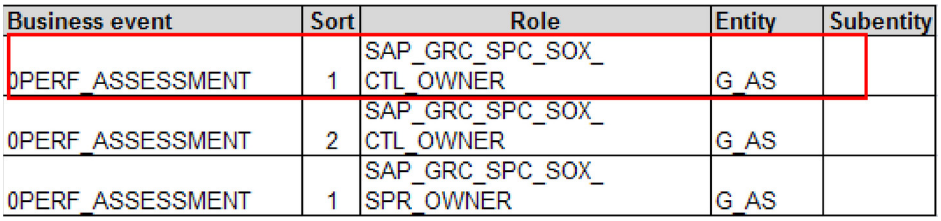
- **Entity** and **subentity** are optional. You can leave them empty. You only need to include them in cases to differentiate the business events. In the following example, Perform Signoff and Perform AOD do not need entities or subentities because the task can only be performed in one way. Perform Assessment is differentiated so that control owner performs Control Design assessment (CD) and subprocess owner performs Process Design assessment (PD).



Business event	Sort	Role	Entity	Subentity
0PERF_ASSESSMENT	1	SAP_GRC_SPC_CTL_OWNER	G_AS	CD
0PERF_ASSESSMENT	2	SAP_GRC_SPC_SP_OWNER	G_AS	PD
0PERF_SIGNOFF	1	SPC_GRC_SPC_ORG_OWNER		
0PERF_AOD	2	SPC_GRC_SPC_ORG_OWNER		

Figure 5

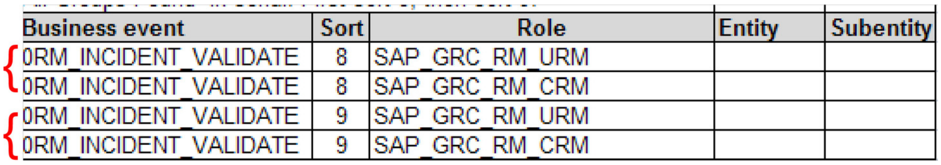
- For all business events (except for Incident_Validate and Master_Data_Change_Notify), the application processes the business events on the basis of **first group** found. In the following example, the application processes the first group found (Sort 1) for the Perf_Assessment business event and stops.



Business event	Sort	Role	Entity	Subentity
0PERF_ASSESSMENT	1	SAP_GRC_SPC_SOX_CTL_OWNER	G_AS	
0PERF_ASSESSMENT	2	SAP_GRC_SPC_SOX_CTL_OWNER	G_AS	
0PERF_ASSESSMENT	1	SAP_GRC_SPC_SOX_SPR_OWNER	G_AS	

Figure 6

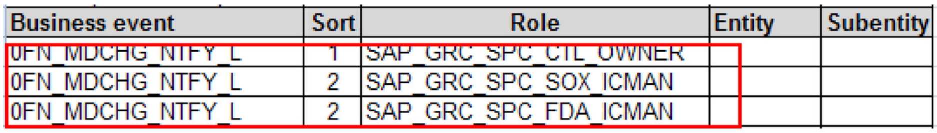
- The Incident_Validate business event is processed in **serial** for **All Groups Found**. The following example illustrates that the application first processes the sort 8 group, then the sort 9 group.



Business event	Sort	Role	Entity	Subentity
0RM_INCIDENT_VALIDATE	8	SAP_GRC_RM_URM		
0RM_INCIDENT_VALIDATE	8	SAP_GRC_RM_CRM		
0RM_INCIDENT_VALIDATE	9	SAP_GRC_RM_URM		
0RM_INCIDENT_VALIDATE	9	SAP_GRC_RM_CRM		

Figure 7

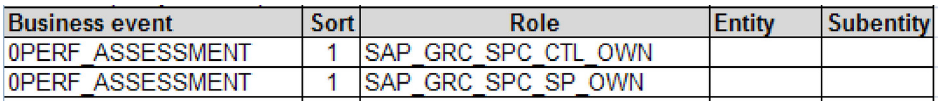
- The MasterData_Change_Notification business event is processed in **parallel** for **All Groups Found**, The following example illustrates the notification is sent to the control owner, SOX internal control manager, and FDA internal control manager concurrently.



Business event	Sort	Role	Entity	Subentity
0FN_MDCHG_NTFY_L	1	SAP_GRC_SPC_CTL_OWNER		
0FN_MDCHG_NTFY_L	2	SAP_GRC_SPC_SOX_ICMAN		
0FN_MDCHG_NTFY_L	2	SAP_GRC_SPC_FDA_ICMAN		

Figure 8

- You can specify a backup role to receive the workflow task by placing different roles in the same sort group with the same business event. The following example illustrates that, because the control owner role is lower in the entity hierarchy, it is processed first. However, if there is no user assigned to that role, the task is assigned to the subprocess owner.



Business event	Sort	Role	Entity	Subentity
0PERF_ASSESSMENT	1	SAP_GRC_SPC_CTL_OWN		
0PERF_ASSESSMENT	1	SAP_GRC_SPC_SP_OWN		

Figure 9

- These business events must be configured as follows:
  - 0PC_RECE_ISSUE

    When the subentity is CO or MO, enter the entity as G_IS. For other all other subentities, enter the entity as G_AS.
  - 0PC_RECE_REM_PLAN

    Enter the entity as G_IS (issue); the entity of the remediation plan creator.
  - 0PC_PERF_SIGNOFF and 0PC_PERF_AOD

    Enter the entity as **ORGUNIT**, not SIGNOFF.

More Information

SAP Delivered Business Events in *Appendix A: PC and RM*

5.4 Ticket Based Authorizations

The information in this section applies to both Process Control and Risk Management. Most users have the authorizations to complete their assigned work item. However, sometimes it is required to pass on a work item to a user who does not have the required authorizations. Ticket Based Authorizations provides temporary authorizations to the user to enable them to complete the work item. Once the work item has been completed, or reassigned to another user, the ticket expires for this user.

> Note
>
> The delivered ticket based authorizations cannot be modified. Further, the functionality is transparent to the user. This information is provided for explanatory purposes only.

Users Who May Need Ticket Based Authorizations

- Process Control users:
  - Assessment Performer

    - Assessment Reviewer
    - Effectiveness Tester
    - Test Reviewer
    - Issue Owner
    - Remediation Owner
    - Any user who needs to assign a workflow task to substitution or to the next processor.
- Risk Management users:
    - Risk survey performer
    - Activity survey performer
    - KRI survey performer

Time Related Aspects

- Once a user starts to perform the task from the work inbox, the authorization is given to the user.
- The authorization is temporary. A user who no longer holds the ticket is no longer authorized to perform the task.
- The authorization expires when the task is submitted. If the time has passed beyond the task due date, but the user has not submitted the task, the authorization remains active.
- The authorization is subject to the SAP Business Workflow escalation functionality.

5.5 Authorization Objects Relevant to Security

The information in this section applies to Process Control and Risk Management. You must maintain the Process Control and Risk Management authorizations for application server objects:

- **Personnel Planning (PLOG)** from Organizational Management:

  The general object type **Organization** (orgunit) is used in Process Control and Risk Management.

  > Note
  > - Organizations created in other projects are also available in Process Control and Risk Management.
  > - Organizations created in Process Control and Risk Management are available in other projects.

- **Case Management** and **Records Management**:
    - The Process Control assessments, tests, issues, and remediation plans are stored in Case or Records Management. The RMS ID for Process Control is GRPC_PC.
    - The Risk Management analysis, responses, and surveys are stored in Case or Records Management. The RMS ID for Risk Management is GRRM_RM.

5.6 Authorization Objects Relevant to Enterprise Search and ODP

The following authorization objects are relevant to Enterprise Search and Operation Data Provisioning (ODP).

Enterprise Search

- GRFN_ES

  This authorization object controls the access to enterprise search. It has the element Entity.

Operation Data Provisioning

- GRFN_ODP

  This authorization object checks for access to GRC entities via ODP. The following are the defined fields:
  - GRC_ENTITY — The GRC entity (or object type) to which the authorization entry corresponds.
  - GRFN_OBJ — The IDs of objects which the user can access.
- GRFN_ODP_C

  This authorization object does an authority check for access to GRC entities with IDs via ODP. The following are the defined fields:
  - GRC_ENTITY — The GRC entity (or object type) to which the authorization entry corresponds.
  - GRFN_OBJ_C — The Complex IDs of objects which the user can access.
- GRFN_ODP_E

  This authorization object checks for access to GRC entities via ODP. The following is the defined field:
  - GRC_ENTITY — The GRC entity (or object type) to which the authorization entry corresponds.
- GRFN_ODP_R

  This authorization object does an authority check for access to GRC regulation-specific entities via ODP. The following are the defined fields:
  - GRC_ENTITY — The GRC entity (or object type) to which the authorization entry corresponds.
  - GRFN_OBJ — The IDs of objects which the user can access.
  - GRPC_REG — Regulation object ID
- GRFN_ODPRC

  This authorization object does an authority check for access to GRC regulation-specific entities with complex IDs via ODP. The following are the defined fields:
  - GRC_ENTITY — The GRC entity (or object type) to which the authorization entry corresponds.
  - GRFN_OBJ_C — The Complex IDs of objects which the user can access.
  - GRPC_REG — Regulation object ID.

6 Application Security: Access Control

The information in this section applies to only Access Control. This section explains the application authorizations model and concepts. Access Control leverages the standard SAP NetWeaver, SAP NetWeaver Application Server ABAP, and SAP NetWeaver Portal user management and authorization. The security information for SAP NetWeaver, SAP NetWeaver Application Server ABAP, and SAP NetWeaver Portal also apply.

For information about SAP NetWeaver, SAP NetWeaver Application Server ABAP, and SAP NetWeaver Portal see the SAP NetWeaver, SAP NetWeaver Application Server ABAP, and SAP NetWeaver Portal security guides.

Prerequisites

You have knowledge of the following tools, terms, and concepts:

- ABAP Application Server
  - Customizing activities (transaction SPRO)
  - PFCG
  - SU01
- Portal
  - User Administration
  - Content Administration
  - Portal Roles
- Business Client
  - Menu of PFCG roles

For more information about Access Control concepts and features, see the *SAP Access Control 10.1 Application Help* at help.sap.com/grc-ac.

A user's access to screens and menus on the front-end is determined by the following:

- The applications that are installed
- The role type
- The authorizations granted to the role type

Application Authorizations

The following table lists examples of screens on the front-end you see based on the **applications** installed on your system:

Table 21

Item	Application
My Home › *Work Inbox*	All
My Home › *My Delegation* › *Approver Delegation*	SAP Access Control
Global Compliance Structure › *Indirect Entity-Level Controls*	SAP Process Control
Assessments › *Proposed Risks and Risk Evaluations*	SAP Risk Management

For more information about the information architecture for the screens and menus delivered by SAP, see the *Appendix*.

Customizing Front-end Screens and Menus

You can configure user-specific front-end screens and menus in the Customizing activities accessed from the SPRO transaction.

> ⚠ Caution
>
> SAP does not recommend you customize the information architecture because if SAP provides updates to the content, then such changes update only the standard SAP-delivered repository and Launchpads. The changes do not directly update any customized versions.

You carry out the configuration activities from the transaction SPRO, *SAP Reference IMG* > *Governance, Risk, and Compliance* > *General Settings* > *Maintain Customer Specific Menus*. Modify

Maintain Authorizations for Applications Links and *Configure LaunchPad for Menus* according to your user's needs..

Privacy Concerns

Notify your users as required by your company's privacy policy that user information such as first Name, last Name, E-mail address, roles, and other personal information is stored by the program GRAC_REPOSITORY_OBJECT_SYNC.

Maintaining Authorizations

Access Control uses object level authorizations. Authorizations are granted to users based on the authorizations of specific roles and the authorization objects assigned to those roles. To maintain the authorizations, you use PFCG and the information in this guide about the delivered roles and authorization objects.

SAP provides a set of sample roles for Access Control, which include recommended authorizations. You can create your own PFCG roles or copy the sample roles to your customer namespace. Then modify them as needed.

6.1 Delivered Roles

Access Control leverages the SAP NetWeaver authorization model and assigns authorizations to users based on roles. The following sample roles are delivered with the application. You must copy them into your own namespace to use them.

Table 22

Feature	Role Name	Description
All AC	SAP_GRAC_ALL	Super administrator for Access Control. ℹ Note You must assign this role to the WF-BATCH user.

Feature	Role Name	Description
All AC	SAP_GRAC_BASE	Gives basic authorizations required for all AC users. You must assign this role to all AC users.
All AC	SAP_GRAC_REPORTS	Ability to run all AC reports and have the display access for all drill-downs.
All AC	SAP_GRAC_NWBC	Gives the authorizations to launch NWBC. You must assign this role to all AC users.
All AC	SAP_GRAC_SETUP	Gives authorizations to set up and customize AC.
All AC	SAP_GRAC_DISPLAY_ALL	Gives display-only access to all master data and application data.
Role management	SAP_GRAC_ROLE_MGMT_USER	Role management business user
Role management	SAP_GRAC_ROLE_MGMT_DESIGNER	Role management designer
Role management	SAP_GRAC_ROLE_MGMT_ROLE_OWNER	The Role Management role owner
Access request	SAP_GRAC_ACCESS_REQUESTER	The role for the access request end user
Access request	SAP_GRAC_ACCESS_APPROVER	The role for the access request approver
Access request	SAP_GRAC_ACCESS_REQUEST_ADMIN	The role for the access request administrator
Emergency Access management	SAP_GRAC_SUPER_USER_MGMT_ADMIN	Emergency Access management administrator for centralized firefighting
Emergency Access management	SAP_GRAC_SUPER_USER_MGMT_OWNER	Emergency Access management owner
Emergency Access management	SAP_GRAC_SUPER_USER_MGMT_CNTLR	Emergency Access management controller
Emergency Access management	SAP_GRAC_SUPER_USER_MGMT_USER	Emergency Access management firefighter for centralized firefighting
Emergency Access management	SAP_GRIA_SUPER_USER_MGMT_ADMIN	Emergency Access management administrator for plug-in firefighting
Emergency Access management	SAP_GRIA_SUPER_USER_MGMT_USER	Emergency Access management firefighter for plug-in firefighting
Access risk analysis	SAP_GRAC_RULE_SETUP	This role has the authorization to define access rules
Access risk analysis	SAP_GRAC_RISK_ANALYSIS	This role has the authorization to perform access risk analysis

Feature	Role Name	Description
Access risk analysis	`SAP_GRAC_ALERTS`	This role has the authorization to generate, clear and delete access risk alerts
Access risk analysis	`SAP_GRAC_CONTROL_OWNER`	This role has the authorization to create mitigating controls.
Access risk analysis	`SAP_GRAC_RISK_OWNER`	This role has the authorization to run access risk maintenance and access risk analysis.
Access risk analysis	`SAP_GRAC_CONTROL_MONITOR`	This role has the authorization to run risk analysis, mitigating control assignment, and assign mitigating controls to an access risk.
Access risk analysis	`SAP_GRAC_CONTROL_APPROVER`	This role is used for control and control assignments. It has the authorization to run risk analysis, mitigating control assignment, and workflow approval for access risk alerts.
Access risk analysis	`SAP_GRAC_FUNCTION_APPROVER`	This role is the delivered agent for workflow in access control. It has authorization to approve, create, read, update, and delete workflow requests.
Workflow	`SAP_GRC_MSMP_WF_ADMIN_ALL`	Administrator role for MSMP workflows
Workflow	SAP_GRC_MSMP_WF_CONFIG_ALL	Configurator role for MSMP workflows

6.2 Authorization Object Names

Access Control authorizations for roles are maintained by the assignment of authorization objects.

> Note
>
> For use with Fiori fact sheets, verify that the following authorization objects are in place: Mitigation Control – GRAC-MITC, Role – GRAC-ROLED, Risk – GRAC-RISK, User – GRAC-USER

The table lists the authorization objects delivered with the application:

Table 23

Object		Description
1	GRAC_ACTN	This object grants the authorization to perform different actions.
2	GRAC_ALERT	This object allows you to generate, clean up, and create alerts.

Object		Description
3	GRAC_ASIGN	The object allows you to assign owner types to firefighter IDs.
4	GRAC_BPROC	The object allows you to create, read, update, and delete business processes, and to assign business processes to risks and functions.
5	GRAC_BGJOB	The object allows you to execute background jobs.
6	GRAC_CGRP	This object allows to maintain an Access Control Custom Group.
7	GRAC_CPROF	The object allows you to create, read, update, and delete SoD critical profiles.
8	GRAC_CROLE	The object allows you to create, read, update, and delete SoD critical roles.
9	GRAC_EMPLY	The object allows you to restrict activities based on the following attributes: cost center, department, company, location. You use this object to maintain authorization for attributes not in the in the GRAC_USER object.
10	GRAC_FFOBJ	The object allows you to restrict creation of FFID or FFROLE based on system user ID, system, or activity.
11	GRAC_FFOWN	The object allows you to create, read, update, and delete FFID owners based on the owner type, user ID, or system ID.
12	GRAC_FUNC	The object allows you to maintain authorizations for the SoD function based on the following attributes: activity, function ID, action (SOD transaction), and permission.
13	GRAC_HROBJ	The object allows you to restrict activities for the HR object based on specific attributes: activity, connector ID, HR object type, HR object ID.
14	GRAC_MITC	The object allows you to maintain mitigation controls.
15	GRAC_ORGRL	The object allows you to maintain SoD organization rules.

Object		Description
16	GRAC_OUNIT	The object allows you to maintain org units for access control.
17	GRAC_OWNER	The object allows you to maintain owners in access control.
18	GRAC_PROF	The object allows you to maintain the SoD profile.
19	GRAC_RA	The object allows you to perform risk analysis. You can specify if the user has authorizations to only execute risk analysis, or has administrator rights.
20	GRAC_RCODE	The object allows you to maintain the reason code.
21	GRAC_REP	The object allows you to excute all reports.
22	GRAC_REQ	The object allows you to maintain access requests.
23	GRAC_RISK	The object allows you to maintain SoD access risk.
24	GRAC_RLMM	The object allows you to perform role mass maintenance.
25	GRAC_ROLED	This object allows you to enforce authorizations for accessing roles during role definition.
26	GRAC_ROLEP	This object allows you to control which roles a user can request.
27	GRAC_ROLER	This object allows you to perform role risk analysis.
28	GRAC_RSET	The object allows you to create, read, update, and delete SoD rule sets.
29	GRAC_SUPP	The object allows you to create, read, update, and delete SoD supplementary rules.
30	GRAC_SYS	The object allows you authorize access to specific connectors or systems based on application type and system ID.
31	GRAC_SYSTM	This object allows system level access to Access Control.
32	GRAC_USER	The object allows you to restrict activities based on the following

Object		Description
		attributes: user group, user ID, connector, user group, orgunit.
33	GRFN_CONN	This object allows you to access connectors in CCITS (the GRC integration engine).

7 Appendix A: Process Control and Risk Management

The information in this section applies to both Process Control and Risk Management.

7.1 Delivered Roles and Relevant Authorization Objects

These are the delivered back-end roles for Process Control and Risk Management. You assign the roles to configure user permissions and authorizations.

Table 24

Role ID	Application	Description
SAP_GRC_FN_ALL	Process Control Risk Management	This is the power user role. The role can access both the front-end and back-end systems. It does not use entity-level security and therefore bypasses the authorizations from the SAP_GRC_FN_BUSINESS_USER role. ➔ Recommendation This role provides extensive access. For security purposes, we recommend you only use the role in emergencies such as troubleshooting task issues. It includes the following authorizations: • Administration functions in Process Control and Risk Management Customizing • Structure setup in expert mode • Data upload for structure setup • Central Delegation — Delegation to any user in the system. i Note The role does not contain the authorizations for customizing workflows, case management, or Web services activation. For these authorizations in: • Process Control, use SAP_GRC_SPC_CUSTOMIZING. • Risk Management, use SAP_GRC_RM_CUSTOMIZING.

Role ID	Application	Description
SAP_GRC_FN_BASE	Process Control Risk Management	This technical role is required for all users to access the application.
SAP_GRC_FN_BUSINESS_USER	Process Control Risk Management	This is the default role assigned to all users. You must assign additional entity-level authorizations to users to enable them to perform activities and act on objects in the application. The role can only access the application through the portal. **Note** Users who set up master data must be assigned additional rights to perform uploads using program GRPCB_UPLOAD.
SAP_GRC_FN_DISPLAY	Process Control Risk Management	This role can access the SAP NetWeaver ABAP Server. This role contains the display authorizations for Customizing and entity level authorizations. **Recommendation** Assign this role to external auditors to give them display access throughout the application. This role bypasses the SAP_GRC_FN_BUSINESS_USER role to grant display authorizations in the back-end. If you wish to have more control over what is displayed, use the SAP_GRC_FN_BUSINESS_USER instead.
SAP_GRC_RM_CUSTOMIZING	Risk Management	This role can access the SAP NetWeaver ABAP Server. This role contains all authorizations for Customizing settings in the application. This includes authorization objects for the following: ● SAP Risk Management ● Customizing Workflow ● Case management ● RFC connections ● Shared objects monitor ● Client comparison with Customizing Cross-system Viewer ● Job scheduling ● E-mail notification settings ● Web service activation **Note** You may be required to record all your changes in the Customizing request. Review the client settings in

Role ID	Application	Description
		transaction SCC4 and make sure you have a request available for you, or you are authorized to create one. Note This role does not have authorizations to perform the following tasks: ● Activating and creating BAdI implementations ● SAP NetWeaver Business Intelligence integration ● Remote Logon to configure the RFC connections
SAP_GRC_SPC_CHIP_VIEWER	Process Control Risk Management	This role grants the authority to view entry pages and side panels that are implemented with CHIPs (Collaborative Human Interface Part).

Role ID	Application	Description
SAP_GRC_SPC_CUSTOMIZING	Process Control	This role can access the SAP NetWeaver ABAP Server. This role contains all authorizations for Customizing settings in the application. This includes authorization objects for the following: • SAP Process Control • Customizing Workflow • Case management • RFC connections • Shared objects monitor • Client comparison with Customizing Cross-system Viewer • Job scheduling • E-mail notification settings • Web service activation Note You may be required to record all your changes in the Customizing request. Review the client settings in transaction SCC4 and make sure you have a request available for you, or you are authorized to create one. Note This role does not have authorizations to perform the following tasks: • Activating and creating BAdI implementations • SAP NetWeaver Business Intelligence integration • Remote Logon to configure the RFC connections
SAP_GRC_SPC_SCHEDULER	Process Control	This role grants the authority to perform background job execution.
SAP_GRC_SPC_SETUP	Process Control	This role grants the authority for system setup and installation.

For more information, see the individual roles in the IMG.

PFCG Basic Role Authorization Objects

SAP delivers the following authorization objects for the PFCG basic roles:

- **GRFN_USER**
  This authorization object is used to separate business users and power users, and controls the access to perform your own or central delegation. It has only the Activity element.
- **GRFN_CONN**
  This authorization object is used to run automated rules testing or monitoring on other systems. It grants **Remote Function Call** authority to the user. To assign this authorization to users, use transaction SU01 in

the back-end system to create a new role, add the authorization object to the role, and assign the role to users.

7.2 SAP Delivered Business Events

Business events are the placeholders for recipient determination in workflow driven scenarios. When the workflow needs to determine the recipient, it uses the correlated object of the workflow instance and business event.

SAP ships default rules for recipient determination based on the entity, activity, and datapart used in roles. You can overwrite the default rules with your own rules by using the direct mapping of the business events and their roles.

For information about the delivered business events and where they are used in the application, view the BC Set for the Customizing activity *Maintain Custom Agent Determination Rules*, under *Governance, Risk, and Compliance* › *General Settings* › *Workflow*.

The following table provides a list of the SAP delivered business events and a description:

Table 25

Business Event	Business Event Name	Description
0FN_AHISSUE_DEFAULT_PRC	Default processor for Ad hoc issue	When an ad hoc issue is reported on an object, the application enters the default issue owner. This business event suggests the default ad hoc issue owner.
0FN_AM_BRFP_NOTIFY	CM Event BRFplus notification	The Continuous Monitor subscenario `EVENT` supports sending notifications. When users choose the option to find recipients by `customer agent rule`, this business event supports the determining the recipient.
0FN_ISSUE_NOTIFY	Send notification to object owner of Ad-hoc Issue	When an ad hoc issue is confirmed, the application automatically sends a notification to the object owner. This business event determines the recipient based on the object owner.
0FN_MDCHG_APPR	Get master data change approver who has the change authority of the object	The business event determines the recipient of a change request for master data changes.
0FN_MDCHG_NTFY	Get notified person who has the display authority of the object	The business event determines the recipients of a notification when a master data change happens.
0FN_MDCHG_NTFY_L	Get notified person who has the display authority of the object on local object level	The business event defines the recipients of a notification when a local master data change happens.

Business Event	Business Event Name	Description
0FN_POLICY_APPROVE	Approve policy	This business event determines the recipients to approve policy, when policy is sent for approval . Additionally the agent of 0FN_POLICY_DEFAULT_APPR is also in the recipient list.
0FN_POLICY_DEFAULT_APPR	Default approver for policy	This business event determines the recipients to approve policy, when policy is sent to approve.
0FN_POLICY_REVIEW	Review policy	This business event determines the recipients to review policy.
0PC_CONTROL_PROPOSAL_APPR	Get control proposal approver who has the change authority of the object	This business event determines the approval recipients of the control proposed from PC & and RM integration scenario.
0PC_PERF_AOD	Perform aggregation of deficiencies	This business event determines the recipients of Control Risk Assessment as it can be scheduled in the planner.
0PC_PERF_ASSESSMENT	Perform assessment	This business event determines the recipients of several Assessments as it can be scheduled in the planner.
0PC_PERF_CRA	Perform control risk assessment	This business event determines the recipients of Control Risk Assessments as it can be scheduled in the planner.
0PC_PERF_IELC_ASSESSMENT	Perform indirect Entity-Level Control Assessment	This business event determines the recipients of Indirect Entity-Level Control Assessment as it can be scheduled in the planner.
0PC_PERF_IELC_TESTING	Perform Indirect Entity-Level Control Testing	This business event determines the recipients of `Indirect Entity-Level Control Testing` .
0PC_PERF_RISK_ASSESSMENT	Perform risk assessment	This business event determines the recipients of Risk Assessment.
0PC_PERF_SIGNOFF	Perform Sign-Off	This business event determines the recipients of Sign-Off.
0PC_PERF_TESTING	Perform testing	This business event determines the recipients of Testing.
0PC_RECE_ESCALATION	Receive escalations of workflow	The user is able to configure escalation recipients for overdue workflow items. For more information, see Customizing for *Workflow E-Mail Notification* under

Business Event	Business Event Name	Description
		Governance, Risk and Compliance ▸ *General Settings* ▸ *Workflow* ▸.
0PC_RECE_ISSUE	Default issue owner	This business event determines the recipients of `monitoring` issues. When users manually assign the issue owner, this business event determines the default issue owner.
0PC_RECE_REM_PLAN	Default Remediation Plan Owner	When users manually assign the remediation plan owner, this business event determines the default one.
0PC_VALI_ASSESSMENT	Review assessment	This business event determines the recipients to review assessments.
0PC_VALI_CAPA_EXEC	Review CAPA execution	This business event determines the recipients to review CAPA execution.
0PC_VALI_CAPA_PLAN	Review CAPA plan	This business event determines the recipients to review CAPA plans.
0PC_VALI_CRA	Review control risk assessment	This business event determines the recipients to review Control Risk Assessment.
0PC_VALI_IELC_ASSESSMENT	Review Entity-Level Control Assessment	This business event determines the recipients to review indirect Entity-Level Control Assessment.
0PC_VALI_IELC_TESTING	Review Indirect Entity-Level Control Testing	This business event determines the recipients to review Indirect Entity-Level Control Testing.
0PC_VALI_RISK_ASSESSMENT	Review risk assessment	This business event determines the recipients to review Risk Assessments.
0PC_VALI_TESTING	Review manual testing	This business event determines the recipients to review testing for manual controls.
0RM_ACTIVITY_SURVEY	Activity Survey	This business event determines the recipients of the activity survey.
0RM_ACTIVITY_VALIDATE	Activity Validation	This business event determines the recipients of the activity validation .
0RM_COLLAB_ASSMNT_SUB	Contribute to Collaborative Risk Assessment	This business event determines all recipients of the initial workflow or survey to participate in a collaborative risk assessment.
0RM_COLLAB_ASSMNT_TOP	Consolidate Collaborative Risk Assessment	This business event determines the consolidator of a collaborative risk

Business Event	Business Event Name	Description
		assessment. This user receives a workflow item that allows them to track the progress of the collaborative risk assessment. Once the assessment is finished they get another workflow item to start the consolidation of the results.
0RM_INCIDENT_VALIDATE	Incident Validation	After an Incident has been created and submitted, or posted from outside, the validation workflow is triggered. This business event determines multiple groups of validators for the incident. First a validation workflow item goes out to all members of the first group. Once a member of the first group has approved the incident the members of the next group receive a validation item, and so on. The incident is completely approved after a member from each group has approved it. If it is sent to rework by anyone, the validation cycle begins again with the first group again.
0RM_KRI_LIAISON	KRI Liaison	This business event is used to determine the workflow recipients for KRI implementation requests and KRI localization requests. A KRI implementation request is triggered after a new KRI implementation request has been created for a KRI template. A localization request is triggered when a localization for a KRI instance is requested on the risk management front end.
0RM_KRI_NOTIFICATION	KRI Notification	This business event determines the recipients for the notification of violated business rules maintained for one or multiple KRI instances on the risk management front end.
0RM_KRI_SURVEY	Risk Indicator Survey	This business event determines the recipients of the risk indicator survey
0RM_OPP_ASSESSMENT	Opportunity Assessment	This business event determines the recipients of the opportunity assessment.

Business Event	Business Event Name	Description
0RM_OPP_VALIDATE	Opportunity Validation	This business event determines the recipients of the opportunity validation.
0RM_RESP_AHISSUE_UPDATE	Response update from issue status change	The business event determines the recipients of an e-mail notification when response completeness reaches 100% based on related issue closing.
0RM_RESP_CONT_UPDATE	Response update from Control's cases	The business event determines the recipients of an e-mail notification when response completeness or effectiveness is changed based on related control rating change.
0RM_RESP_POLICY_UPDATE	Response update from policy status change	The business event determines the recipients of an e-mail notification when response completeness reached 100% based on related policy status change.
0RM_RESPONSE_UPDATE	Response Validation	This business event determines the recipients of the response update.
0RM_RISK_ASSESSMENT	Risk Assessment	This business event determines the recipients of the risk assessment.
0RM_RISK_PROPOSE	Risk Proposal	After a risk is proposed in SAP Risk Management, a workflow is sent to a risk management expert to validate the proposal. If it is accepted, a new risk is created for it. This business event determines approver.
0RM_RISK_SURVEY	Risk Survey	This business event determines the recipients of the risk survey
0RM_RISK_VALIDATE	Risk Validation	This business event determines the recipients of the risk validation.

7.3 SAP Delivered Workflow Recipient BC Set (Process Control)

The information in this section applies to only Process Control. The use of this BC set is optional. Risk Management uses the default agent determination rules and does not have a BC set.

Process Control is delivered with the following agent determination rule BC sets:

- **Cross Regulations**

Table 26

Business Event	Sort	Role	Entity	Subentity
0FN_AHISSUE_DEFAULT_PRC	1	SAP_GRC_SPC_CRS_CTL_OWNER	CONTROL	Not applicable
0FN_AHISSUE_DEFAULT_PRC	1	SAP_GRC_SPC_CRS_ICMAN	CORPORATE	Not applicable
0FN_AHISSUE_DEFAULT_PRC	1	SAP_GRC_SPC_CRS_POLICY_OWNER	POLICY	Not applicable
0FN_AHISSUE_DEFAULT_PRC	1	SAP_GRC_SPC_CRS_PRC_OWNER	PROCESS	Not applicable
0FN_AHISSUE_DEFAULT_PRC	1	SAP_GRC_SPC_CRS_SPR_OWNER	SUBPROCESS	Not applicable
0FN_AHISSUE_DEFAULT_PRC	1	SAP_GRC_SPC_GLOBAL_ORG_OWNER	ORGUNIT	Not applicable
0FN_AHISSUE_DEFAULT_PRC	1	SAP_GRC_SPC_GLOBAL_REG_ADMIN	REGULATION	Not applicable
0FN_AHISSUE_DEFAULT_PRC	2	SAP_GRC_SPC_GLOBAL_ORG_OWNER	ECONTROL	Not applicable
0FN_AM_BRFP_NOTIFY	1	SAP_GRC_SPC_CRS_CTL_OWNER	CONTROL	Not applicable
0FN_ISSUE_NOTIFY	1	SAP_GRC_SPC_CRS_CTL_OWNER	CONTROL	Not applicable
0FN_ISSUE_NOTIFY	1	SAP_GRC_SPC_CRS_ICMAN	CORPORATE	Not applicable
0FN_ISSUE_NOTIFY	1	SAP_GRC_SPC_CRS_POLICY_OWNER	POLICY	Not applicable
0FN_ISSUE_NOTIFY	1	SAP_GRC_SPC_CRS_PRC_OWNER	PROCESS	Not applicable
0FN_ISSUE_NOTIFY	1	SAP_GRC_SPC_CRS_SPR_OWNER	SUBPROCESS	Not applicable
0FN_ISSUE_NOTIFY	1	SAP_GRC_SPC_GLOBAL_ORG_OWNER	ORGUNIT	Not applicable
0FN_ISSUE_NOTIFY	1	SAP_GRC_SPC_GLOBAL_REG_ADMIN	REGULATION	Not applicable
0FN_ISSUE_NOTIFY	2	SAP_GRC_SPC_GLOBAL_ORG_OWNER	ECONTROL	Not applicable
0FN_POLICY_DEFAULT_APPR	1	SAP_GRC_SPC_GLOBAL_ORG_OWNER	Not applicable	Not applicable

Business Event	Sort	Role	Entity	Subentity
0FN_POLICY_APPROVE	1	SAP_GRC_SPC_CRS_PLC_APPR	Not applicable	Not applicable
0FN_POLICY_REVIEW	1	SAP_GRC_SPC_CRS_PLC_REVIEW	Not applicable	Not applicable
0PC_CONTROL_PROPOSAL_APPR	1	SAP_GRC_SPC_CRS_SPR_OWNER	Not applicable	Not applicable
0PC_CONTROL_PROPOSAL_APPR	2	SAP_GRC_SPC_CRS_SPR_OWNER	Not applicable	Not applicable
0PC_CONTROL_PROPOSAL_APPR	3	SAP_GRC_SPC_GLOBAL_ORG_OWNER	Not applicable	Not applicable
0PC_PERF_AOD	1	SAP_GRC_SPC_GLOBAL_ORG_OWNER	ORGUNIT	Not applicable
0PC_PERF_ASSESSMENT	1	SAP_GRC_SPC_CRS_SPR_OWNER	G_AS	PD
0PC_PERF_CRA	1	SAP_GRC_SPC_CRS_SPR_OWNER	G_AS	CR
0PC_PERF_IELC_ASSESSMENT	1	SAP_GRC_SPC_GLOBAL_ORG_OWNER	G_AS	MCOU
0PC_PERF_IELC_ASSESSMENT	2	SAP_GRC_SPC_GLOBAL_INT_AUD	G_AS	MCOU
0PC_PERF_IELC_TESTING	2	SAP_GRC_SPC_GLOBAL_INT_AUD	G_TL	MTOU
0PC_PERF_RISK_ASSESSMENT	1	SAP_GRC_SPC_GLOBAL_ORG_OWNER	G_AS	RISK
0PC_PERF_RISK_ASSESSMENT	2	SAP_GRC_SPC_GLOBAL_INT_AUD	G_AS	RISK
0PC_PERF_SIGNOFF	1	SAP_GRC_SPC_GLOBAL_ORG_OWNER	ORGUNIT	Not applicable
0PC_PERF_SIGNOFF	2	SAP_GRC_SPC_GLOBAL_CEO_CFO	ORGUNIT	Not applicable
0PC_RECE_ESCALATION	1	SAP_GRC_SPC_CRS_SPR_OWNER	CONTROL	Not applicable
0PC_RECE_ESCALATION	3	SAP_GRC_SPC_CRS_PRC_OWNER	G_AS	CE
0PC_RECE_ESCALATION	4	SAP_GRC_SPC_GLOBAL_CEO_CFO	G_AS	MCOU

Business Event	Sort	Role	Entity	Subentity
0PC_RECE_ESCALATION	5	SAP_GRC_SPC_GLOBAL_INT_AUD	G_AS	CR
0PC_RECE_ESCALATION	6	SAP_GRC_SPC_GLOBAL_CEO_CFO	G_AS	RISK
0PC_RECE_ESCALATION	8	SAP_GRC_SPC_CRS_PRC_OWNER	G_AS	CD
0PC_RECE_ESCALATION	10	SAP_GRC_SPC_CRS_PRC_OWNER	G_IS	CO
0PC_RECE_ESCALATION	11	SAP_GRC_SPC_CRS_SPR_OWNER	G_IS	MO
0PC_RECE_ESCALATION	12	SAP_GRC_SPC_CRS_SPR_OWNER	G_IS	CE
0PC_RECE_ESCALATION	13	SAP_GRC_SPC_CRS_SPR_OWNER	G_IS	TE
0PC_RECE_ESCALATION	16	SAP_GRC_SPC_CRS_PRC_OWNER	G_IS	PD
0PC_RECE_ESCALATION	17	SAP_GRC_SPC_CRS_PRC_OWNER	G_TL	TE
0PC_RECE_ESCALATION	18	SAP_GRC_SPC_CRS_SPR_OWNER	G_TL	CO
0PC_RECE_ESCALATION	19	SAP_GRC_SPC_GLOBAL_ORG_OWNER	G_TL	MTOU
0PC_RECE_ESCALATION	20	SAP_GRC_SPC_GLOBAL_INT_AUD	ORGUNIT	Not applicable
0PC_RECE_ISSUE	1	SAP_GRC_SPC_CRS_PRC_OWNER	G_AS	PD
0PC_RECE_ISSUE	1	SAP_GRC_SPC_CRS_SPR_OWNER	G_IS	CO
0PC_RECE_ISSUE	2	SAP_GRC_SPC_CRS_SPR_OWNER	G_AS	CD
0PC_RECE_ISSUE	3	SAP_GRC_SPC_CRS_SPR_OWNER	G_AS	CE
0PC_RECE_ISSUE	4	SAP_GRC_SPC_CRS_SPR_OWNER	G_TL	TE
0PC_RECE_ISSUE	5	SAP_GRC_SPC_CRS_SPR_OWNER	G_TL	CO

Business Event	Sort	Role	Entity	Subentity
0PC_RECE_REM_PLAN	1	SAP_GRC_SPC_CRS_SPR_OWNER	G_IS	PD
0PC_RECE_REM_PLAN	1	SAP_GRC_SPC_GLOBAL_ORG_OWNER	G_IS	MCOU
0PC_RECE_REM_PLAN	2	SAP_GRC_SPC_GLOBAL_INT_AUD	G_IS	MCOU
0PC_RECE_REM_PLAN	3	SAP_GRC_SPC_GLOBAL_INT_AUD	G_IS	MTOU
0PC_VALI_ASSESSMENT	1	SAP_GRC_SPC_CRS_PRC_OWNER	G_AS	PD
0PC_VALI_ASSESSMENT	1	SAP_GRC_SPC_CRS_SPR_OWNER	G_AS	CD
0PC_VALI_ASSESSMENT	2	SAP_GRC_SPC_CRS_SPR_OWNER	G_AS	CE
0PC_VALI_CAPA_EXEC	1	SAP_GRC_SPC_FDA_CAPA_EXEC_APPR	G_CP	Not applicable
0PC_VALI_CAPA_PLAN	1	SAP_GRC_SPC_FDA_CAPA_PLAN_APPR	G_CP	Not applicable
0PC_VALI_TESTING	1	SAP_GRC_SPC_CRS_SPR_OWNER	G_TL	TE

- **SOX Regulation**

Table 27

Business Event	Sort	Role	Entity	Subentity
0FN_AM_BRFP_NOTIFY	1	SAP_GRC_SPC_SOX_CTL_OWNER	CONTROL	Not applicable
0PC_PERF_AOD	2	SAP_GRC_SPC_SOX_ICMAN	ORGUNIT	Not applicable
0PC_PERF_ASSESSMENT	1	SAP_GRC_SPC_SOX_CTL_OWNER	G_AS	CD
0PC_PERF_ASSESSMENT	2	SAP_GRC_SPC_SOX_CTL_OWNER	G_AS	CE
0PC_PERF_IELC_TESTING	1	SAP_GRC_SPC_SOX_ORG_TESTER	G_TL	MTOU
0PC_PERF_TESTING	1	SAP_GRC_SPC_SOX_PRC_TESTER	G_TL	CO
0PC_PERF_TESTING	2	SAP_GRC_SPC_SOX_PRC_TESTER	G_TL	TE

Business Event	Sort	Role	Entity	Subentity
0PC_RECE_ESCALATION	2	SAP_GRC_SPC_SOX_ICMAN	CPROPOSAL	Not applicable
0PC_RECE_ESCALATION	7	SAP_GRC_SPC_SOX_ICMAN	G_AS	PD
0PC_RECE_ESCALATION	14	SAP_GRC_SPC_SOX_ICMAN	G_IS	MCOU
0PC_RECE_ESCALATION	15	SAP_GRC_SPC_SOX_ICMAN	G_IS	MTOU
0PC_RECE_EVENT_NOTIFICATION	1	SAP_GRC_SPC_SOX_CTL_OWNER	CONTROL	Not applicable
0PC_RECE_ISSUE	1	SAP_GRC_SPC_SOX_CTL_OWNER	G_IS	MO
0PC_RECE_ISSUE	1	SAP_GRC_SPC_SOX_ICMAN	G_AS	MCOU
0PC_RECE_ISSUE	2	SAP_GRC_SPC_SOX_ICMAN	G_TL	MTOU
0PC_RECE_REM_PLAN	1	SAP_GRC_SPC_SOX_CTL_OWNER	G_IS	CD
0PC_RECE_REM_PLAN	1	SAP_GRC_SPC_SOX_ORG_TESTER	G_IS	MTOU
0PC_RECE_REM_PLAN	2	SAP_GRC_SPC_SOX_CTL_OWNER	G_IS	CE
0PC_RECE_REM_PLAN	3	SAP_GRC_SPC_SOX_CTL_OWNER	G_IS	TE
0PC_RECE_REM_PLAN	4	SAP_GRC_SPC_SOX_CTL_OWNER	G_IS	CO
0PC_RECE_REM_PLAN	5	SAP_GRC_SPC_SOX_CTL_OWNER	G_IS	MO
0PC_VALI_CRA	1	SAP_GRC_SPC_SOX_ICMAN	G_AS	CR
0PC_VALI_IELC_ASSESSMENT	1	SAP_GRC_SPC_SOX_ICMAN	G_AS	MCOU
0PC_VALI_IELC_TESTING	1	SAP_GRC_SPC_SOX_ICMAN	G_TL	MTOU
0PC_VALI_RISK_ASSESSMENT	1	SAP_GRC_SPC_SOX_ICMAN	G_AS	RISK

- **FDA Regulation**

Table 28

Business Event	Sort	Role	Entity	Subentity
0FN_AM_BRFP_NOTIFY	1	SAP_GRC_SPC_FDA_CTL_OWNER	CONTROL	Not applicable
0PC_PERF_ASSESSMENT	2	SAP_GRC_SPC_FDA_CTL_OWNER	G_AS	CE
0PC_PERF_TESTING	1	SAP_GRC_SPC_FDA_PRC_TESTER	G_TL	CO
0PC_PERF_TESTING	2	SAP_GRC_SPC_FDA_PRC_TESTER	G_TL	TE
0PC_RECE_ESCALATION	2	SAP_GRC_SPC_FDA_ICMAN	CPROPOSAL	Not applicable
0PC_RECE_ESCALATION	9	SAP_GRC_SPC_FDA_ICMAN	G_CP	Not applicable
0PC_RECE_EVENT_NOTIFICATION	1	SAP_GRC_SPC_FDA_CTL_OWNER	CONTROL	Not applicable
0PC_RECE_ISSUE	1	SAP_GRC_SPC_FDA_CTL_OWNER	G_IS	MO
0PC_RECE_REM_PLAN	1	SAP_GRC_SPC_FDA_CTL_OWNER	G_IS	CE
0PC_RECE_REM_PLAN	2	SAP_GRC_SPC_FDA_CTL_OWNER	G_IS	TE
0PC_RECE_REM_PLAN	3	SAP_GRC_SPC_FDA_CTL_OWNER	G_IS	CO
0PC_RECE_REM_PLAN	4	SAP_GRC_SPC_FDA_CTL_OWNER	G_IS	MO

If you want to implement a SOX initiative using the delivered BC Sets, active Cross Regulation and SOX.

If you want to implement an FDA initiative using the delivered BC Sets, active Cross Regulation and FDA.

If you want to implement both SOX and FDA initiatives using the delivered BC Sets, active Cross Regulation, SOX, and FDA.

7.4 Authorization Object Elements

The information in this section applies to both the process control application and risk management application.

You configure the authorizations for application roles by maintaining the authorization object elements. The following tables list the descriptions of the authorization object elements. For information about the procedure, see *Maintaining Application Roles*.

7.4.1 Activity

The following activities are relevant for both process control and risk management applications.

Activity controls the user behavior on the business object.

Table 29

Activity	Authorization Object
CHANGE	GRFN_API
CREATE	GRFN_API
DELETE	GRFN_API
DISPLAY	GRFN_API
ANALYZE	GRFN_REP
PRINT	GRFN_REP
DISPLAY TAKEOVER	GRFN_USER
DISTRIBUTE	GRFN_USER
EXECUTE	GRFN_CONN

7.4.2 Entities

The entity specifies the business object. Its values are all the business objects within the application. The table lists the authorization relevant entities for the process control and risk management applications:

Table 30

Entity	Application	Description	Central
ACC_GROUP	Process Control	Account Group	X
ACTIVITY	Risk Management	Activity	not applicable
AM_JOB	Process Control Risk Management	Scheduler	not applicable
AM_JOBP	Process Control Risk Management	Job Log	not applicable
AM_JOBRESULT	Process Control Risk Management	Job Result	not applicable
AM_AHQRY	Process Control Risk Management	Ad-Hoc Query	not applicable
AM_EVENT	Process Control Risk Management	Event Monitor	not applicable
AOD	Process Control	AOD	not applicable

Entity	Application	Description	Central
BR	Process Control Risk Management	Business Rule	not applicable
BRA	Process Control Risk Management	Business Rule Assignment	not applicable
CACTIVITY	Risk Management	Activity Category	X
CAGROUP	Risk Management	Activity Category Group	X
COBJECTIVE	Process Control	Control Objective	X
COGROUP	Risk Management	Opportunity Category	X
CONTROL	Process Control Risk Management	Control	not applicable
COPP	Risk Management	Central Opportunity	X
CPROPOSAL	Process Control	Control Proposal	not applicable
CRGROUP	Process Control Risk Management	Risk Category	X
CRISK	Process Control Risk Management	Central Risk	X
ECGROUP	Process Control	Indirect Entity-Level Control Group	not applicable
ECONTROL	Process Control	Indirect Entity-Level Control	not applicable
EO	Process Control Risk Management	Data Source	not applicable
EVENT	Process Control	Event	X
EVENT_D	Process Control	Dispatched Event	X
EXEC	Process Control	Scheduler	X
G_AS	Process Control	Assessment	not applicable
G_CP	Process Control	CAPA Plan	not applicable
G_IS	Process Control	Issue	not applicable
G_PL	Process Control	Remediation plan	not applicable
G_TL	Process Control	Test Log	not applicable
INCIDENT	Risk Management	Incident	not applicable
JOBLOG	Process Control	Job log from Scheduler	X
JOBRESULT	Process Control	Job Result	X
KRIIMPL	Risk Management	KRI Implementation	X

Entity	Application	Description	Central
KRIIMPLREQ	Risk Management	KRI Implementation Request	X
KRIINST	Risk Management	KRI Instance	not applicable
KRIRULE	Risk Management	KRI Business Rule	not applicable
KRITMPL	Risk Management	KRI Template	X
OBJECTIVE	Risk Management	Objectives	X
OLSP	Process Control	OLSP	X
OPP	Risk Management	Opportunity	not applicable
ORGUNIT	Process Control Risk Management	Organization	not applicable
PLANNER	Process Control Risk Management	Planner	not applicable
PRISK	Risk Management	Risk Proposal	not applicable
PROCESS	Process Control	Process	not applicable
QSURVEY	Risk Management	Question Survey	X
REGULATION	Process Control Risk Management	Regulation/Policy	X
REG_GROUP	Process Control Risk Management	Regulation/Policy Group	X
REG_REQ	Process Control Risk Management	Regulation/Policy Requirement	X
RESPONSE	Risk Management	Response	not applicable
RISK	Process Control Risk Management	Risk	not applicable
RULCR	Process Control	Rule Criteria	X
RULE	Process Control	Rule	X
SAPQUERY	Process Control	SAP Query	X
SCRIPT	Process Control	Rule Script	X
SIGNOFF	Process Control	Sign-Off	not applicable
SRV_QUESTION	Process Control Risk Management	Survey Question	X
SUBPROCESS	Process Control	Subprocess	not applicable
SURVEY	Process Control Risk Management	Survey Template	X

Entity	Application	Description	Central
TESTPLAN	Process Control	Testplan	X
XCONTROL	Process Control	Central Control	X
XECGROUP	Process Control	Central Indirect Entity-Level Control Group	X
XECONTROL	Process Control	Central Indirect Entity-Level Control	X
XPROCESS	Process Control	Central Process	X
XSUBPROCESS	Process Control	Central Subprocess	X

7.4.3 Subentities

The information in this section is relevant for both process control and risk management applications:

Subentities are the subgroup of objects related to an entity. Not all entities have subentities. The table lists the subentities and related entities:

Table 31

Entity	Subentity	Description
G_AS	CD	Control Design Assessment
G_AS	CE	Self Assessment
G_AS	CR	Control Risk Assessment
G_AS	MCOU	Indirect ELC Assessment
G_AS	PD	Sub Process Assessment
G_AS	RISK	Risk Assessment
G_CP	CE	CAPA plan for Self Assessment
G_CP	CO	CAPA plan for Compliance Test
G_CP	MO	CAPA plan for Monitoring Test
G_CP	TE	CAPA plan for Manual Test
G_IS	CD	Control Design Assessment Issue
G_IS	CE	Self Assessment Issue
G_IS	CO	Compliance Test Issue
G_IS	MCOU	Indirect ELC Assessment Issue
G_IS	MO	Monitoring Test Issue
G_IS	MTOU	Indirect ELC Test Issue

Entity	Subentity	Description
G_IS	PD	Sub Process Assessment Issue
G_IS	TE	Manual Test Issue
G_PL	CD	Control Design Assessment Plan
G_PL	CE	Self Assessment Plan
G_PL	CO	Compliance Test Plan
G_PL	MCOU	Indirect ELC Assessment Plan
G_PL	MO	Monitoring Test Plan
G_PL	MTOU	Indirect ELC Test Plan
G_PL	PD	Sub Process Assessment Plan
G_PL	TE	Manual Test Plan
G_TL	CO	Compliance Test Test Log
G_TL	MO	Monitoring Test Test Log
G_TL	MTOU	Indirect ELC Test Test Log
G_TL	TE	Manual Test Test Log
PLANNER	PERF-AOD	Perform Aggregation of Deficiencies
PLANNER	PERF-CDASS	Perform Control Design Assessment
PLANNER	PERF-CEASS	Perform Self Assessment
PLANNER	PERF-CRISK	Perform Control Risk Assessment
PLANNER	PERF-ETEST	Perform Indirect ELC Test
PLANNER	PERF-MCAOU	Perform Indirect ELC Assessment
PLANNER	PERF-PDASS	Perform Sub Process Assessment
PLANNER	PERF-RISK	Perform Risk Assessment
PLANNER	PERF-SOFOU	Perform Sign-Off
PLANNER	PERF-TEST	Perform Test
PLANNER	PERF-PLCA	Perform Policy Acknowledgement
PLANNER	PERF-PLCQ	Perform Policy Quiz
PLANNER	PERF-PLCS	Perform Policy Survey
PLANNER	GRRM_ACT	Perform Activity Validation
PLANNER	GRRM_ANAL	Perform Risk Assessment
PLANNER	GRRM_OPP	Perform Opportunity Assessment
PLANNER	GRRM_OPPVA	Perform Opportunity Validation

Entity	Subentity	Description
PLANNER	GRRM_RESP	Perform Responsible Validation
PLANNER	GRRM_RISK	Perform Risk Validation
PLANNER	GRRM_SACT	Perform Activity Survey
PLANNER	GRRM_SKRI	Perform Risk Indicator Survey
PLANNER	GRRM_SRISK	Perform Risk Survey

7.4.4 Dataparts

The information in this section is relevant for both process control and risk management applications.

Table 32

Entity	Datapart	Description	Relevant Application
ACTIVITY	DATA	Activity Details	Risk management
ACTIVITY	VALIDATE	Activity Validation	Risk management
BR	STATUS	Business Rule Status	Process control Risk management
CONTROL	CDATA	Additional data of control	Process control
CONTROL	DATA	Basic data of control	Process control
CONTROL	RISK	Assignment of control to risk	Process control
CONTROL	RULE	Assignment of control to rule	Process control
CONTROL	TDATA	Test attributes of control	Process control
ECONTROL	DATA	Basic data of indirect Entity-Level Control	Process control
ECONTROL	TDATA	Test attributes of indirect Entity-Level Control	Process control
INCIDENT	DATA	Maintain Incident Draft	Risk management
INCIDENT	REWORK	Rework Incident (resubmit or refuse)	Risk management
INCIDENT	VALIDATE	Validate Incident (validate or send to rework)	Risk management
KRITMPL	DATA	KRI Template Data	Risk management
KRITMPL	LIAISON	KRI Liaison	Risk management
OPP	DATA	Opportunity Details	Risk management
OPP	VALIDATE	Opportunity Validation	Risk management

Entity	Datapart	Description	Relevant Application
ORGUNIT	DATA	Orgunit Data	Risk management Process control
ORGUNIT	ECONTROL	Assignment of Indirect Entity Level Control	Process control
ORGUNIT	INSCOPE	Orgunit Scoping Information	Process control
ORGUNIT	RISK_ASSESSMENT	Risk Assessment on Organizations	Risk management
ORGUNIT	ROLES	Role Assignment on Organizations	Risk management Process control
ORGUNIT	ROLES_PC	Role Assignment on Processes, Subprocesses, and Controls	Process control
ORGUNIT	ROLES_RM	Role Assignment on Risks and Activities	Risk management
ORGUNIT	SIGNOFF	Sign-Off	Process control
ORGUNIT	SUBPROCESS	Assignment of Subprocess	Process control
RESPONSE	DATA	Response Data Part	Risk management
RESPONSE	VALIDATE	Response Validation	Risk management
RISK	DATA	Risk Details	Process control Risk management
RISK	VALIDATE	Risk Validation	Risk management
SUBPROCESS	COR_GLOB	Assignment of global control to subprocess, control objective, and risk	Process control
SUBPROCESS	COR_ORG	Assignment of referenced control to subprocess, control objective and risk	Process control
SUBPROCESS	DATA	Local subprocess attributes	Process control
SUBPROCESS	INSCOPE	Subprocess Scoping Information	Process control
XCONTROL	DATA	Basic data of control	Process control
XCONTROL	TDATA	Test attributes of control	Process control
XECONTROL	DATA	Basic data of indirect Entity-Level Control	Process control
XECONTROL	TDATA	Test attributes of indirect Entity-Level Control	Process control

8 Appendix B: Access Control

The information in this section applies only to SAP Access Control. It contains the details about the delivered roles, authorization objects, and authorization fields.

8.1 Delivered Roles and Relevant Authorization Objects

This section lists the delivered Access Control roles and the relevant authorization objects.

8.1.1 Roles Relevant Across All Features

The roles delivered by Access Control are relevant to specific features, such as risk management, emergency access management, and so on. This section covers the roles that are relevant to all Access Control features. The following table lists the delivered roles and the relevant authorization objects:

Table 33

Role	Objects
SAP_GRAC_ALL	• GRAC_ALERT • GRAC_ASIGN • GRAC_BGJOB • GRAC_BPROC • GRAC_CGRP • GRAC_CPROF • GRAC_CROLE • GRAC_EMPLY • GRAC_FFOWN • GRAC_FUNC • GRAC_HROBJ • GRAC_MITC • GRAC_ORGRL • GRAC_OUNIT • GRAC_OWNER • GRAC_PROF • GRAC_RA • GRAC_RCODE • GRAC_REP

Role	Objects
	- GRAC_RISK - GRAC_RLMM - GRAC_ROLED - GRAC_ROLEP - GRAC_ROLER - GRAC_RSET - GRAC_SUPP - GRAC_SYS - GRAC_SYSTM - GRAC_USER - GRFN_CONN
SAP_GRAC_BASE	- GRAC_BGJOB - GRAC_REQ - GRAC_USER - S_START
SAP_GRAC_DISPLAY_ALL	- GRAC_CPROF - GRAC_CROLE - GRAC_EMPLY - GRAC_FFOBJ - GRAC_FFOWN - GRAC_FUNC - GRAC_HROBJ - GRAC_MITC - GRAC_ORGRL - GRAC_OUNIT - GRAC_OWNER - GRAC_PROF - GRAC_RCODE - GRAC_REQ - GRAC_RISK - GRAC_ROLED - GRAC_RSET - GRAC_SUPP - GRAC_SYS - GRAC_SYSTM - GRAC_USER - GRFN_CONN
SAP_GRAC_REPORTS	- GRAC_ALERT

Role	Objects
	- GRAC_ASIGN - GRAC_BPROC - GRAC_CPROF - GRAC_CROLE - GRAC_EMPLY - GRAC_FFOBJ - GRAC_FFOWN - GRAC_FUNC - GRAC_HROBJ - GRAC_MITC - GRAC_ORGRL - GRAC_OUNIT - GRAC_OWNER - GRAC_PROF - GRAC_RA - GRAC_RCODE - GRAC_REP - GRAC_REQ - GRAC_RISK - GRAC_ROLED - GRAC_ROLER - GRAC_RSET - GRAC_SUPP - GRAC_SYS - GRAC_SYSTM - GRAC_USER - GRFN_CONN

8.1.2 Role Management

The following table lists the delivered roles and the relevant authorization objects for role management.

Table 34

Role Name	Objects
SAP_GRAC_ROLE_MGMT_ADMIN	- GRAC_CPROF - GRAC_CROLE - GRAC_FUNC - GRAC_ORGRL

Role Name	Objects
	• GRAC_OWNER • GRAC_RA • GRAC_REP • GRAC_RISK • GRAC_RLMM • GRAC_ROLED • GRAC_RSET • GRAC_SYS • GRAC_SYSTM • GRAC_SUPP • GRFN_CONN
SAP_GRAC_ROLE_MGMT_DESIGNER	• GRAC_CPROF • GRAC_CROLE • GRAC_FUNC • GRAC_ORGRL • GRAC_OWNER • GRAC_RA • GRAC_REP • GRAC_RISK • GRAC_ROLED • GRAC_RSET • GRAC_SYS • GRAC_SYSTM • GRAC_SUPP • GRFN_CONN
SAP_GRAC_ROLE_MGMT_ROLE_OWNER	• GRAC_REP • GRAC_ROLED • GRAC_SYSTM • GRFN_CONN
SAP_GRAC_ROLE_MGMT_USER	• GRAC_ROLED • GRFN_CONN

8.1.3 Access Request

The following table lists the delivered roles and the relevant authorization objects for access request:

Table 35

Role Name	Objects
SAP_GRAC_ACCESS_APPROVER	• GRAC_CPROF • GRAC_CROLE • GRAC_EMPLY • GRAC_FUNC • GRAC_ORGRL • GRAC_RA • GRAC_REQ • GRAC_RISK • GRAC_ROLED • GRAC_ROLEP • GRAC_RSET • GRAC_SUPP R • GRAC_SYS • GRAC_SYSTM • GRAC_USE
SAP_GRAC_ACCESS_REQUEST_ADMIN	• GRAC_CPROF • GRAC_CROLE • GRAC_EMPLY • GRAC_FUNC • GRAC_ORGRL • GRAC_OWNER • GRAC_RA • GRAC_REP • GRAC_REQ • GRAC_RISK • GRAC_ROLED • GRAC_ROLEP • GRAC_RSET • GRAC_SUPP • GRAC_SYS • GRAC_SYSTM • GRAC_USER
SAP_GRAC_ACCESS_REQUESTER	• GRAC_EMPLY • GRAC_REQ • GRAC_ROLED • GRAC_ROLEP • GRAC_SYS • GRAC_SYSTM

Role Name	Objects
	- GRAC_USER

8.1.4 Emergency Access Management

The following table lists the delivered roles and the relevant authorization objects for centralized emergency access management:

Table 36

Role Name	Objects
SAP_GRAC_SUPER_USER_MGMT_ADMIN	• GRAC_ASIGN • GRAC_OWNER • GRAC_RCODE • GRAC_REP • GRAC_ROLED • GRAC_USER
SAP_GRAC_SUPER_USER_MGMT_CNTLR	• GRAC_ASIGN • GRAC_OWNER • GRAC_REP
SAP_GRAC_SUPER_USER_MGMT_OWNER	• GRAC_ASIGN • GRAC_OWNER • GRAC_RCODE • GRAC_ROLED • GRAC_USER
SAP_GRAC_SUPER_USER_MGMT_USER	• GRAC_RCODE • GRAC_USER • GRFN_CONN

Roles for Decentralized Firefighting

For decentralized (plug-in) firefighting scenarios, the following roles are delivered.

Table 37

Role Name	Authorizations
SAP_GRIA_SUPER_USER_MGMT_ADMIN	`/GRCPI/001` - GRAC Authorization Object to extend FF Validity Period `ACTVT` field value: 70 or * (asterisk)
SAP_GRIA_SUPER_USER_MGMT_USER	Transactions: `/GRCPI/GRIA_EAM` and `SU53`

8.1.5 Access Risk Analysis

The following table lists the delivered roles and the relevant authorization objects for access risk analysis:

Table 38

Role Name	Objects
SAP_GRAC_ALERTS	GRAC_ALERT GRAC_CPROF GRAC_CROLE GRAC_FUNC GRAC_HROBJ GRAC_ORGRL GRAC_PROF GRAC_RA GRAC_REP GRAC_RISK GRAC_ROLED GRAC_ROLER GRAC_RSET GRAC_SUPP GRAC_USER GRFN_CONN
SAP_GRAC_CONTROL_APPROVER	GRAC_ALERT GRAC_CPROF GRAC_CROLE GRAC_FUNC GRAC_HROBJ GRAC_MITC GRAC_ORGRL GRAC_OUNIT GRAC_OWNER GRAC_PROF GRAC_RA GRAC_REP GRAC_RISK GRAC_ROLED GRAC_ROLER GRAC_RSET GRAC_SUPP GRAC_USER

Role Name	Objects
SAP_GRAC_CONTROL_MONITOR	• GRAC_CPROF • GRAC_CROLE • GRAC_FUNC • GRAC_HROBJ • GRAC_MITC • GRAC_ORGRL • GRAC_OUNIT • GRAC_OWNER • GRAC_PROF • GRAC_RA • GRAC_REP • GRAC_RISK • GRAC_ROLED • GRAC_ROLER • GRAC_RSET • GRAC_SUPP • GRAC_USER
SAP_GRAC_CONTROL_OWNER	• GRAC_CPROF • GRAC_CROLE • GRAC_FUNC • GRAC_HROBJ • GRAC_MITC • GRAC_ORGRL • GRAC_OUNIT • GRAC_OWNER • GRAC_PROF • GRAC_RA • GRAC_REP • GRAC_RISK • GRAC_ROLED • GRAC_ROLER • GRAC_RSET • GRAC_SUPP • GRAC_USER
SAP_GRAC_FUNCTION_APPROVER	• GRAC_FUNC • GRAC_SYSTM • GRFN_CONN
SAP_GRAC_RISK_ANALYSIS	• GRAC_CPROF

Role Name	Objects
	• GRAC_CGRP • GRAC_CROLE • GRAC_FUNC • GRAC_HROBJ • GRAC_ORGRL • GRAC_PROF • GRAC_RA • GRAC_REP • GRAC_RISK • GRAC_ROLED • GRAC_ROLER • GRAC_RSET • GRAC_SYSTM • GRAC_SUPP • GRAC_USER • GRFN_CONN
SAP_GRAC_RISK_OWNER	• GRAC_FUNC • GRAC_HROBJ • GRAC_ORGRL • GRAC_OWNER • GRAC_PROF • GRAC_RA • GRAC_REP • GRAC_RISK • GRAC_ROLED • GRAC_ROLER • GRAC_RSET • GRAC_SUPP • GRAC_USER
SAP_GRAC_RULE_SETUP	• GRAC_CPROF • GRAC_CROLE • GRAC_FUNC • GRAC_ORGRL • GRAC_REP • GRAC_RISK • GRAC_RSET • GRAC_SUPP • GRAC_SYS • GRAC_SYSTM

Role Name	Objects
	- GRFN_CONN

8.1.6 Workflow

The following table lists the delivered roles and the relevant authorization objects for workflow:

Table 39

Role Name	Object
SAP_GRC_MSMP_WF_ADMIN_ALL	GRFN_MSMP
SAP_GRC_MSMP_WF_CONFIG_ALL	GRFN_MSMP

8.2 Authorization Objects and Relevant Fields

The authorization objects for Access Control use specific authorization fields.

The following table lists the authorization fields that are available for each authorization object:

Table 40

	Object	Fields
1	GRAC_ACTN	• GRAC_ACTN • GRFNW_PRC
2	GRAC_ALERT	• ACTVT • GRAC_ALRTT
3	GRAC_ASIGN	• ACTVT • GRAC_OWN_T
4	GRAC_BGJOB	• ACTVT • GRAC_BGJOB
5	GRAC_BPROC	• ACTVT • GRAC_BPROC
6	GRAC_CGRP	• ACTVT • GRAC_CGRP
7	GRAC_CPROF	• ACTVT • GRAC_CPROF
8	GRAC_CROLE	• ACTVT • GRAC_CROLE
9	GRAC_EMPLY	• ACTVT

	Object	Fields
		• GRAC_COMP • GRAC_COSTC • GRAC_DEPT • GRAC_LOCTN
10	GRAC_FFOBJ	• ACTVT • GRAC_FFOBJ • GRAC_SYSID
11	GRAC_FFOWN	• ACTVT • GRAC_OWN_T • GRAC_SYSID • GRAC_USER
12	GRAC_FUNC	• ACTVT • GRAC_ACT • GRAC_FUNC • GRAC_PRM
13	GRAC_HROBJ	• ACTVT • GRAC_HROBJ • GRAC_HRTYP • GRAC_SYSID
14	GRAC_MITC	• ACTVT • GRAC_MITC • GRAC_OUNIT
15	GRAC_ORGRL	• ACTVT • GRAC_ORGRL
16	GRAC_OUNIT	• ACTVT • GRAC_OUNIT • GRAC_OUTYP
17	GRAC_OWNER	• ACTVT • GRAC_CLASS • GRAC_OUNIT • GRAC_OWN_T • GRAC_SYSID • GRAC_USER
18	GRAC_PROF	• ACTVT • GRAC_PROF • GRAC_SYSID

	Object	Fields
19	GRAC_RA	• ACTVT • GRAC_OTYPE • GRAC_RAMOD • GRAC_REPT
20	GRAC_RCODE	• ACTVT • GRAC_RSCOD • GRAC_SYSID
21	GRAC_REP	• ACTVT • GRAC_REPID
22	GRAC_REQ	• ACTVT • GRAC_BPROC • GRAC_FNCAR • GRAC_RQFOR • GRAC_RQINF • GRAC_RQTYP
23	GRAC_RISK	• ACTVT • GRAC_BPROC • GRAC_RISK • GRAC_RLVL • GRAC_RSET • GRAC_RTYPE
24	GRAC_RLMM	• ACTVT • GRAC_RLMMT
25	GRAC_ROLED	• GRAC_ACTRD • GRAC_BPROC • GRAC_LDSCP • GRAC_RLSEN • GRAC_RLTYP • GRAC_ROLE
26	GRAC_ROLEP	• ACTVT • GRAC_BPROC • GRAC_OUNIT • GRAC_RLTYP • GRAC_ROLE • GRAC_SYSID
27	GRAC_ROLER	• ACTVT • GRAC_OUNIT

	Object	Fields
		- GRAC_ROLE - GRAC_ROTYP - GRAC_SYSID
28	GRAC_RSET	- ACTVT - GRAC_RSET
29	GRAC_SUPP	- ACTVT
30	GRAC_SYS	- ACTVT - GRAC_APPTY - GRAC_ENVRM - GRAC_SYSID
31	GRAC_SYSTM	- ACTVT - GRACSYSACT - GRAC_SYSID
32	GRAC_USER	- ACTVT - GRAC_CLASS - GRAC_OUNIT - GRAC_SYSID - GRAC_USER - GRAC_UTYPE
33	GRFN_MSMP	Note To allow users to view access request data in reports, you must assign this authorization object and the activity **A5** (display report) to their role.

8.3 Authorization Fields

This section covers the technical names for the authorization fields and their descriptions.

For information about the fields that are relevant for specific authorization objects, see *Authorization Objects and Relevant Fields*.

Table 41

	Field Name	Description
1	GRAC_ACT	Action
2	GRAC_ACTRD	Activities

	Field Name	Description
3	GRAC_ALRTT	Alert type
4	GRAC_APPTY	Application type
5	GRAC_BPROC	Business process
6	GRAC_BSUBP	Subprocess
7	GRAC_CLASS	User group
8	GRAC_COMP	Company
9	GRAC_COSTC	Cost center
10	GRAC_CPROF	Profile name
11	GRAC_CROLE	Role name
12	GRAC_CTRID	SOD control ID
13	GRAC_DEPT	Department
14	GRAC_ENVRM	System environment
15	GRAC_FFOBJ	Description for user ID or role
16	GRAC_FNCAR	Functional area
17	GRAC_FUNC	Function ID
18	GRAC_HROBJ	HR object ID
19	GRAC_HRTYP	HR object type
20	GRAC_LDSCP	Connector group
21	GRAC_LOCTN	Location
22	GRAC_MITC	SOD control ID
23	GRAC_MON	Owner description
24	GRAC_OLVL	Resource extension
25	GRAC_ORGRL	Organization rule ID
26	GRAC_OTYPE	Object types for authorization
27	GRAC_OUNIT	HR object ID
28	GRAC_OUTYP	Object type for assigned organization
29	GRAC_OWN_T	Owner type
30	GRAC_PRM	SOD resource
31	GRAC_PROF	Profile name
32	GRAC_RAMOD	Risk analysis mode
33	GRAC_REPID	Report name

	Field Name	Description
34	GRAC_REPT	Report type
35	GRAC_RISK	Access risk ID
36	GRAC_RLMMT	Type for role mass maintenance
37	GRAC_RLSEN	Role sensitivity
38	GRAC_RLTYP	Role type
39	GRAC_RLVL	SOD risk level
40	GRAC_ROLE	Role name
41	GRAC_ROTYP	Role type for risk analysis
42	GRAC_ROWN	Owner description
43	GRAC_RQFOR	Request for single or multiple user
44	GRAC_RQINF	Request Information
45	GRAC_RQSOD	SOD option for request
46	GRAC_RQTYP	Request type
47	GRAC_RSCOD	Title/Short name
48	GRAC_RSET	Rule set ID
49	GRAC_RTYPE	Access risk type
50	GRAC_SYSID	Connector ID
51	GRAC_USER	User ID
52	GRAC_USRTY	Role type for request approver
53	GRAC_UTYPE	User type

8.4 Values for ACTVT Field

The **ACTVT** field is used by almost every Access Control authorization object. The values you select for the activity field controls the actions the role can perform using the authorization object, such as delete or execute.

Note

The GRAC_ROLED authorization object does not use the ACTVT field; it uses the custom attribute: GRAC_ACTRD. For more information, see Values for GRAC_ACTRD Field [page 82].

The following table lists the values you can select for the activity field based on the authorization object:

Table 42

	Authorization Object	Valid Activity Values
1	GRAC_ALERT	Delete, Execute, Archive, Deactivate
2	GRAC_ASIGN	Create or generate, Change, Display, Delete, Administer
3	GRAC_BPROC	Create or generate, Change, Display, Delete, Execute, Assign
4	GRAC_BGJOB	Create or generate, Display, Delete, Administer
5	GRAC_CGRP	Create or generate, Change, Display, Delete, Execute
6	GRAC_CPROF	Create or generate, Change, Display, Delete, Execute, Assign
7	GRAC_CROLE	Create or generate, Change, Display, Delete, Execute, Assign
8	GRAC_EMPLY	Create or generate, Change, Display, Delete, Execute, Administer, Assign, Copy
9	GRAC_FFOBJ	Create or generate, Change, Display, Delete
10	GRAC_FFOWN	Create or generate, Change, Display, Delete, Archive, Administer
11	GRAC_FUNC	Create or generate, Change, Display, Delete, Execute, Generate, Assign
12	GRAC_HROBJ	Create or generate, Change, Display, Delete, Execute, Assign
13	GRAC_MITC	Create or generate, Change, Display, Delete, Assign
14	GRAC_ORGRL	Create or generate, Change, Display, Delete, Activate or Generate, Execute, Assign
15	GRAC_OUNIT	Create or generate, Change, Display, Delete, Execute, Assign
16	GRAC_OWNER	Create or generate, Change, Display, Delete, Archive, Administer, Assign
17	GRAC_PROF	Create or generate, Change, Display, Delete, Execute, Assign
18	GRAC_RA	Execute, Administer
19	GRAC_RCODE	Create or generate, Change, Display, Delete
20	GRAC_REP	Execute
21	GRAC_REQ	Create or generate, Change, Display, Administer, Copy
22	GRAC_RISK	Create or generate, Change, Display, Delete, Execute, Generate, Assign
23	GRAC_RLMM	Perform
24	GRAC_ROLEP	Assign
25	GRAC_ROLER	Execute, Assign
26	GRAC_RSET	Create or generate, Change, Display, Delete, Execute, Assign
27	GRAC_SUPP	Create or generate, Change, Display, Delete
28	GRAC_SYS	Create or generate, Change, Display, Delete, Execute, Assign

	Authorization Object	Valid Activity Values
29	GRAC_SYSTM	Execute Access Control reports
30	GRAC_USER	Create or generate, Change, Display, Delete, Execute, Assign
31	/GRCPI/001	* (asterisk) or blank (empty)

8.5 Values for GRAC_ACTRD Field

The GRAC_ACTRD field is used by the GRAC_ROLED authorization object for role definition.

The **Ticket Number** functionality in BRM allows you to attach ticket numbers to the workflow for role changes. The V8 value in the GRAC_ACTRD field enables the user to edit and overwrite the ticket number in **all** role methodology steps. Without this value, the user can only enter or change the ticket number when the role is in *Create* mode or in *Completed* status.

Table 43

Authorization Object	Field	Value	Description
GRAC_ROLED	GRAC_ACTRD	V8 - Overwrite Ticket Number	The V8 value enables the user to edit the ticket number in **all** role methodologies.

Typographic Conventions

Table 44

Example	Description
<Example>	Angle brackets indicate that you replace these words or characters with appropriate entries to make entries in the system, for example, “Enter your **<User Name>**”.
▶ *Example* ▶ *Example* ▶	Arrows separating the parts of a navigation path, for example, menu options
Example	Emphasized words or expressions
Example	Words or characters that you enter in the system exactly as they appear in the documentation
www.sap.com	Textual cross-references to an internet address
/example	Quicklinks added to the internet address of a homepage to enable quick access to specific content on the Web
123456	Hyperlink to an SAP Note, for example, SAP Note 123456
Example	• Words or characters quoted from the screen. These include field labels, screen titles, pushbutton labels, menu names, and menu options. • Cross-references to other documentation or published works
`Example`	• Output on the screen following a user action, for example, messages • Source code or syntax quoted directly from a program • File and directory names and their paths, names of variables and parameters, and names of installation, upgrade, and database tools
`EXAMPLE`	Technical names of system objects. These include report names, program names, transaction codes, database table names, and key concepts of a programming language when they are surrounded by body text, for example, `SELECT` and `INCLUDE`
`EXAMPLE`	Keys on the keyboard

www.sap.com