SAP GRC

tutorialspoint

SIMPLY EASY LEARNING

www.tutorialspoint.com

https://www.facebook.com/tutorialspointindia https://twitter.com/tutorialspoint

About the Tutorial

SAP GRC (Governance, Risk and Compliance) solution enables organizations to manage regulations and compliance and remove any risk in managing organizations' key operations. As per changing market situation, organizations are growing and rapidly changing, and inappropriate documents are not acceptable for external auditors and regulators. SAP GRC helps organization to manage their regulations and compliance.

This tutorial will walk you through the different features of SAP GRC.

Audience

This tutorial is designed for all those readers who are willing to learn the basics of SAP GRC. This is also useful for those readers who wish to refresh their knowledge of GRC. SAP Security Consultants and SAP Auditors at all levels can also draw benefits from this tutorial.

Prerequisites

The course is designed for beginners with little or no knowledge of SAP GRC. But you need to have a basic understanding of SAP Basics to make the most of this tutorial.

Disclaimer & Copyright

All the content and graphics published in this e-book are the property of Tutorials Point (I) Pvt. Ltd. The user of this e-book is prohibited to reuse, retain, copy, distribute or republish any contents or a part of contents of this e-book in any manner without written consent of the publisher.

We strive to update the contents of our website and tutorials as timely and as precisely as possible, however, the contents may contain inaccuracies or errors. Tutorials Point (I) Pvt. Ltd. provides no guarantee regarding the accuracy, timeliness or completeness of our website or its contents including this tutorial. If you discover any errors on our website or in this tutorial, please notify us at contact@tutorialspoint.com.

Table of Contents

1. SAP GRC — Overview

SAP Governance, Risk and Compliance solution enables organizations to manage regulations and compliance and remove any risk in managing organizations' key operations. As per changing market situation, organizations are growing and rapidly changing and inappropriate documents, spreadsheets are not acceptable for external auditors and regulators.

SAP GRC helps organization to manage their regulations and compliance and perform the following activities:

- Easy integration of GRC activities into existing process and automating key GRC activities.
- Low complexity and managing risk efficiently.
- Improve risk management activities.
- Managing fraud in business processed and audit management effectively.
- Organizations perform better and companies can protect their values.
- SAP GRC solution consists of three main areas: Analyze, manage and monitor.

Modules in SAP GRC

Let us now understand the different modules in SAP GRC:

SAP GRC Access Control

To mitigate risk in an organization, it is required to perform risk control as part of compliance and regulation practice. Responsibilities should be clearly defined, managing role provisioning and managing access for super user is critical for managing risk in an organization.

SAP GRC Process Control and Fraud Management

SAP GRC Process Control software solution is used for managing compliance and policy management. The compliance management capabilities allow organizations to manage and monitor their internal control environments. Organizations can proactively fix any identified issues and certify and report on the overall state of the corresponding compliance activities.

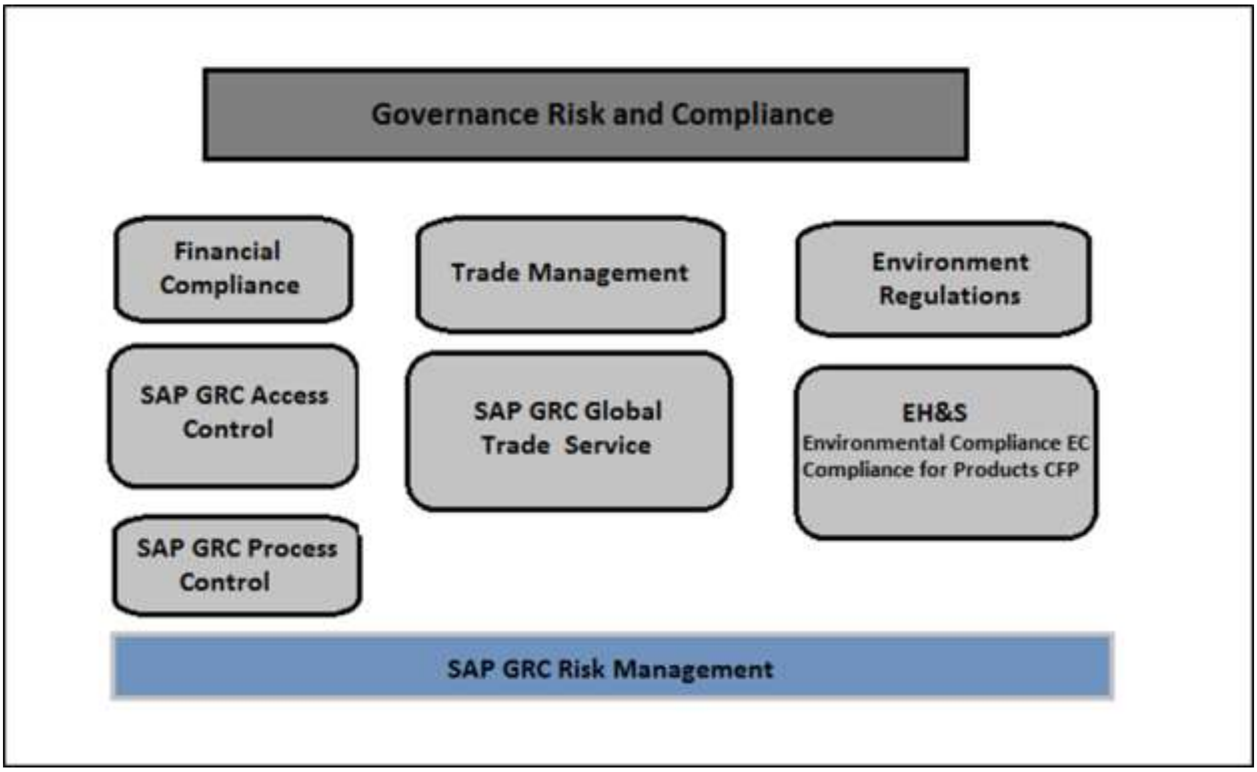
SAP Process control supports the complete life cycle of policy management, including the distribution and adherence of policies by target groups. These policies help organizations to reduce the cost of compliance and improve management transparency and enables organization to develop compliance management processes and policies in business environment.

SAP GRC Risk Management

SAP GRC Risk Management allows you to manage risk management activities. You can do advance planning to identify risk in business and implement measures to manage risk and allow you to make better decision that improves the performance of business.

Risks come in many forms:

- Operational Risk
- Strategic Risk
- Compliance Risk
- Financial Risk



SAP GRC Audit Management

This is used to improve the audit management process in an organization by documenting artifacts, organizing work papers, and creating audit reports. You can easily integrate with other governance, risk and compliance solution and enable organizations to align audit management policies with business goals.

SAP GRC audit management helps auditor in making things simple by providing the following capabilities:

- You can instantly capture the artifacts for audit management and other evidences using mobile capabilities drag-drop feature.

- You can easily create, track, and manage audit issues with global monitoring and follow up.

- You can perform search using search capabilities that allows to get more information from legacy and working papers.

- You can engage auditors with a user-friendly interface and collaboration tools.

- Easy integration of audit management with SAP Fraud Management, SAP Risk Management, and SAP Process Control to align audit process with business goals.

- Quick resolution of issues using automated tracking tool.

- Enhance the staff utilization, and less travel costs resulted from internal audit planning, resource management, and scheduling.

- Easy integration with SAP Business Objects reporting and data visualization tool to visualize audit reports using Lumira and other BI reporting.

- Use of pre-established templates to standardize audit artifacts and reporting process.

SAP GRC Fraud Management

SAP GRC fraud management tool helps organizations to detect and prevent frauds at early stage and hence reducing minimizing the business loss. Scans can be performed on huge amount of data in real time with more accuracy and fraudent activities can be easily identified.

SAP fraud management software can help organizations with following capabilities:

- Easy investigation and documentation of fraud cases.

- Increase the system alert and responsiveness to prevent fraudent activities to happen more frequently in future.

- Easy scanning of high volumes of transactions and business data.

SAP GRC Global Trade Services

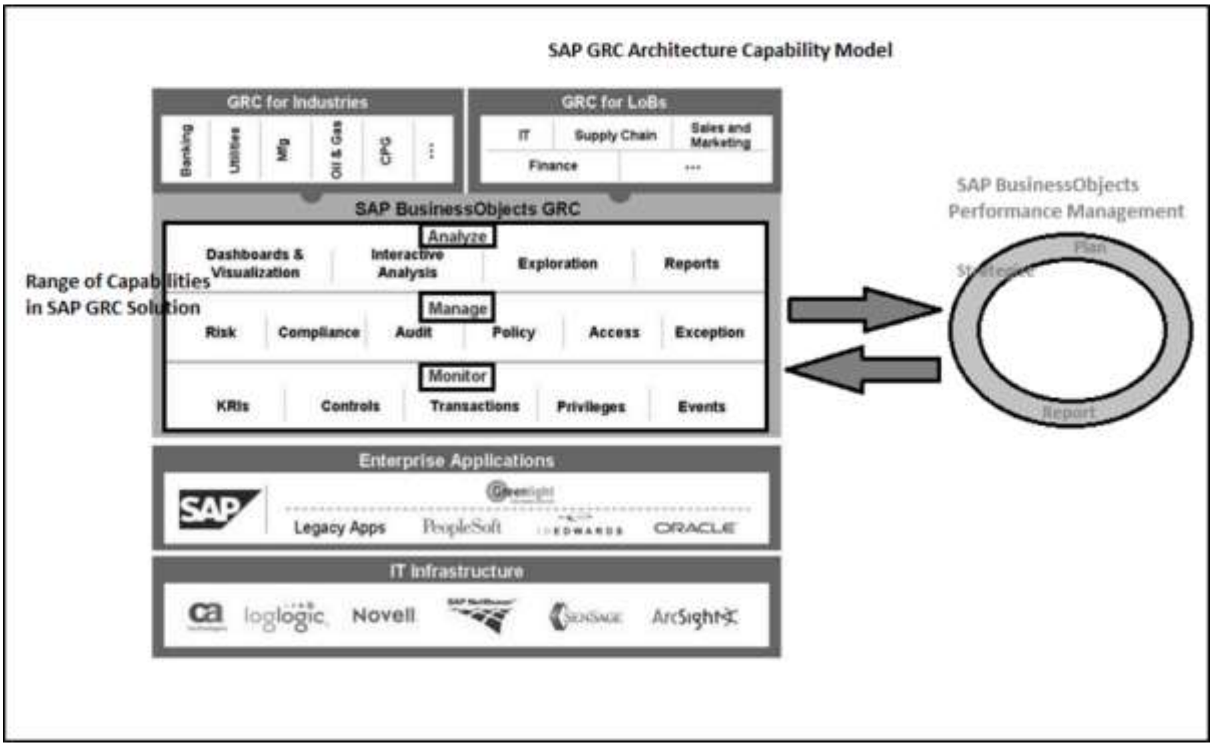
SAP GRC GTS software helps organizations to enhance cross border supply within limits of international trade management. It helps in reducing the penalty of risks from International Trade Regulation authorities.

It provides centralize global trade management process with a single repository for all compliance master data and content irrespective of size of an organization.

SAP GRC Capability Model

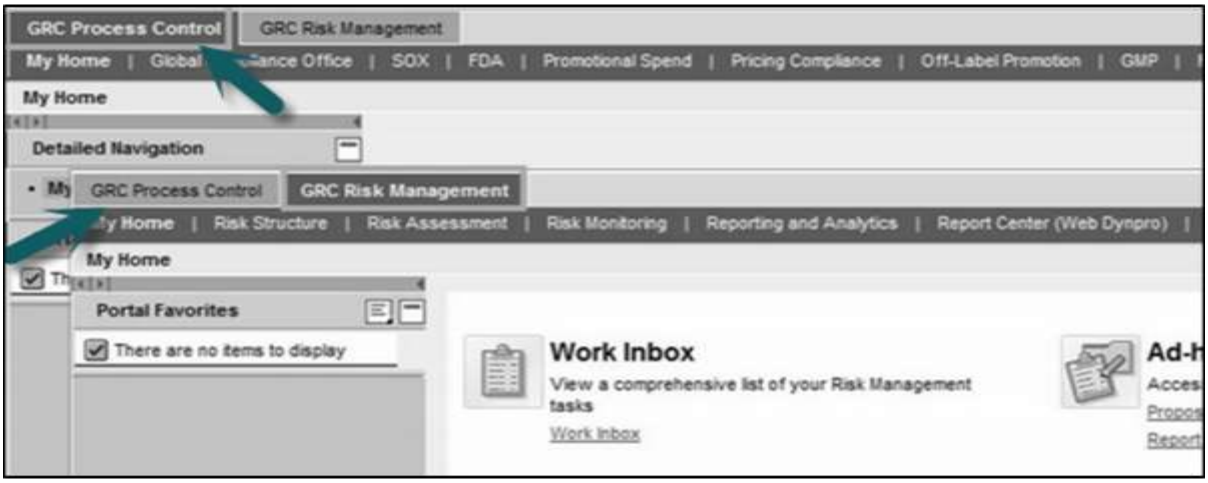
SAP BusinessObjects GRC solution consists of three main capabilities: **Analyze, Manage and Monitor**.

In the following diagram, you can see the SAP GRC Capability Model that covers all the key features of SAP GRC software. Using GRC, organizations can check for all potential risks and compliance findings and can take correct decision to mitigate them.



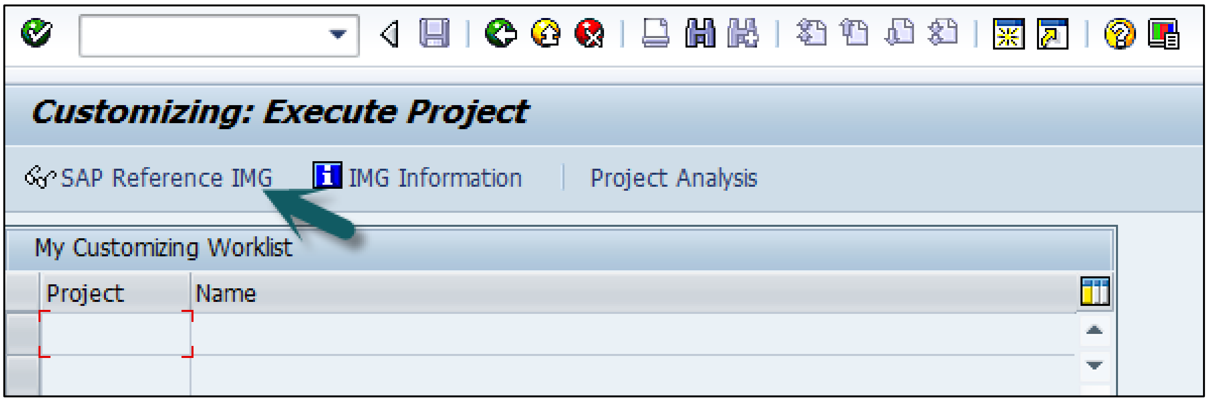
2. SAP GRC — Navigation

In older versions of SAP GRC, to use access control, process control and risk management, there was a separate navigation for each component. This means that users, to perform cross component duties, had to login to each module separately and login multiple times. This resulted in a tough process to manage multiple windows and documents to search was also tough.

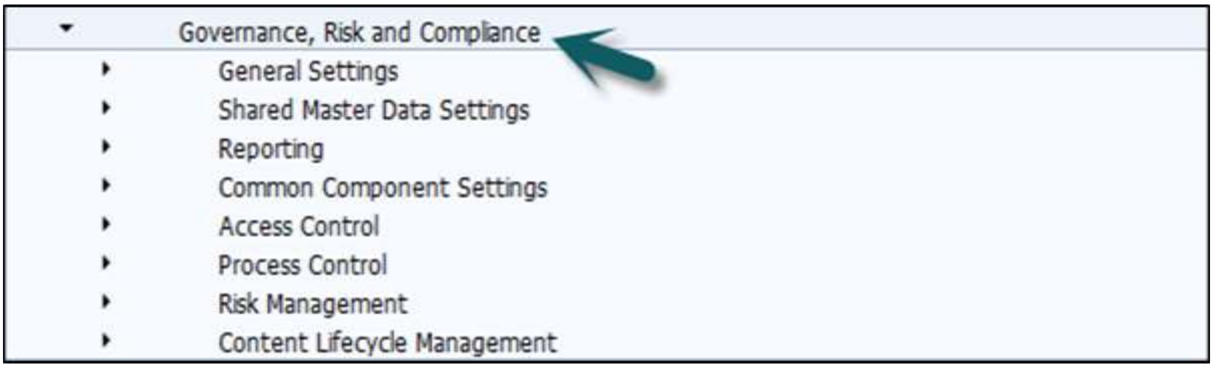

GRC Process Control
GRC Risk Management
My Home | Global ...ance Office | SOX | FDA | Promotional Spend | Pricing Compliance | Off-Label Promotion | GMP |
My Home
Detailed Navigation
My
GRC Process Control
GRC Risk Management
My Home | Risk Structure | Risk Assessment | Risk Monitoring | Reporting and Analytics | Report Center (Web Dynpro) |
My Home
Portal Favorites
There are no items to display
Work Inbox
View a comprehensive list of your Risk Management tasks
Work Inbox
Ad-h
Acces
Propos
Report

SAP GRC 10.0 provides direct navigation to access control, process control and risk management components for a single user as per authorization and removes the management of multiple windows.

Step 1: To perform customizing activities and maintain configuration settings for GRC solution, go to T-code: SPRO -> SAP Reference IMG



Step 2: Expand Governance, Risk and Compliance node:



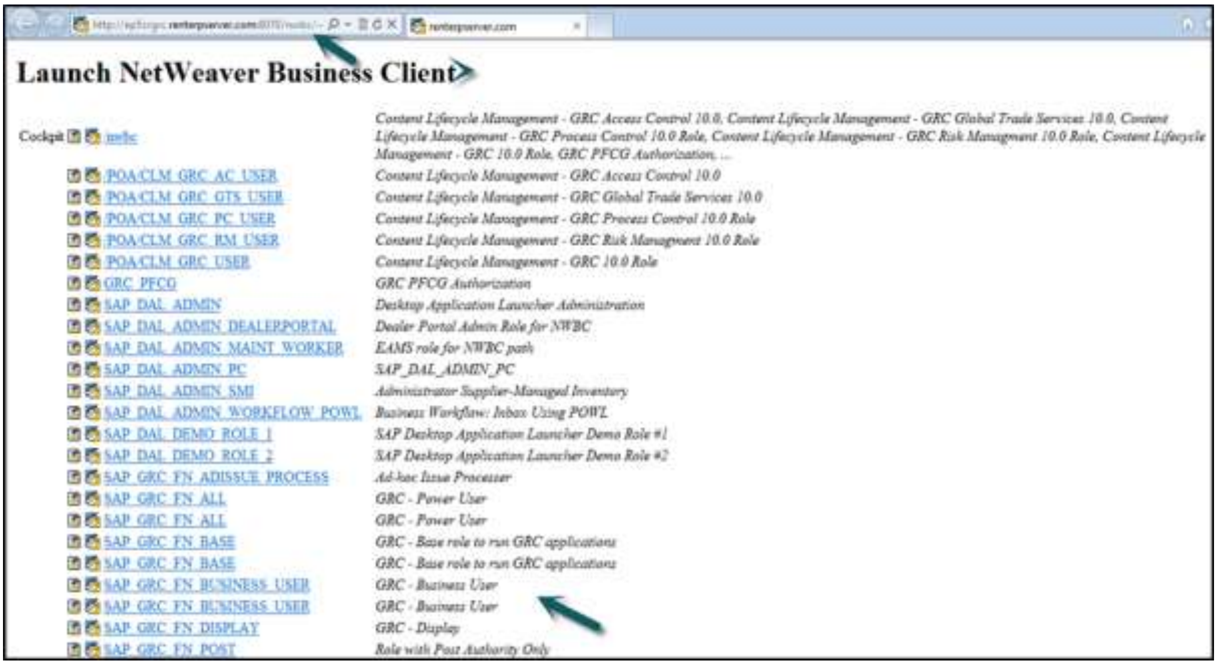
- Governance, Risk and Compliance
  - General Settings
  - Shared Master Data Settings
  - Reporting
  - Common Component Settings
  - Access Control
  - Process Control
  - Risk Management
  - Content Lifecycle Management

Step 3: Logon to NetWeaver Business Client:

Run the transaction for NWBC in SAP Easy access.

It will open NetWeaver Business Client screen and you will receive the following url:

http://ep5crgrc.renterpserver.com:8070/nwbc/~launch/?sap-client=800&sap-language=EN



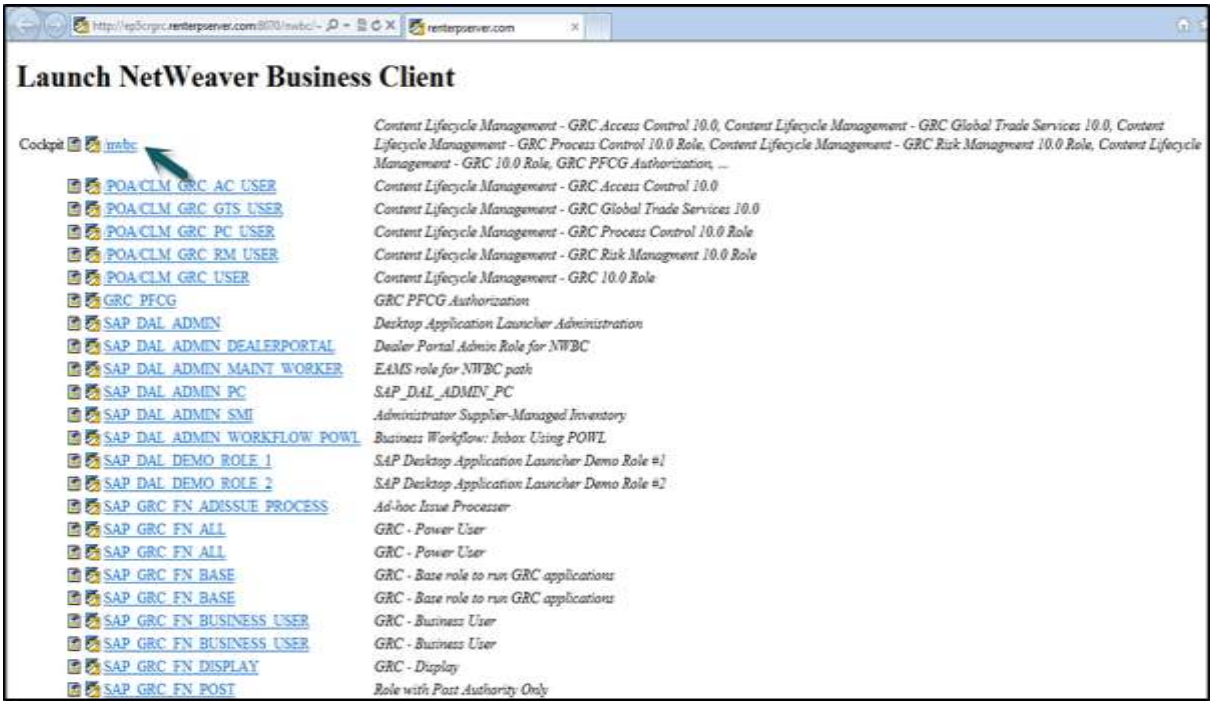
Launch NetWeaver Business Client

Cockpit nwbc	Content Lifecycle Management - GRC Access Control 10.0, Content Lifecycle Management - GRC Global Trade Services 10.0, Content Lifecycle Management - GRC Process Control 10.0 Role, Content Lifecycle Management - GRC Risk Managment 10.0 Role, Content Lifecycle Management - GRC 10.0 Role, GRC PFCG Authorization, ...
POA/CLM_GRC_AC_USER	Content Lifecycle Management - GRC Access Control 10.0
POA/CLM_GRC_GTS_USER	Content Lifecycle Management - GRC Global Trade Services 10.0
POA/CLM_GRC_PC_USER	Content Lifecycle Management - GRC Process Control 10.0 Role
POA/CLM_GRC_RM_USER	Content Lifecycle Management - GRC Risk Managment 10.0 Role
POA/CLM_GRC_USER	Content Lifecycle Management - GRC 10.0 Role
GRC_PFCG	GRC PFCG Authorization
SAP_DAL_ADMIN	Desktop Application Launcher Administration
SAP_DAL_ADMIN_DEALERPORTAL	Dealer Portal Admin Role for NWBC
SAP_DAL_ADMIN_MAINT_WORKER	EAMS role for NWBC path
SAP_DAL_ADMIN_PC	SAP_DAL_ADMIN_PC
SAP_DAL_ADMIN_SMI	Administrator Supplier-Managed Inventory
SAP_DAL_ADMIN_WORKFLOW_POWL	Business Workflow: Inbox Using POWL
SAP_DAL_DEMO_ROLE_1	SAP Desktop Application Launcher Demo Role #1
SAP_DAL_DEMO_ROLE_2	SAP Desktop Application Launcher Demo Role #2
SAP_GRC_FN_ADISSUE_PROCESS	Ad-hoc Issue Processor
SAP_GRC_FN_ALL	GRC - Power User
SAP_GRC_FN_ALL	GRC - Power User
SAP_GRC_FN_BASE	GRC - Base role to run GRC applications
SAP_GRC_FN_BASE	GRC - Base role to run GRC applications
SAP_GRC_FN_BUSINESS_USER	GRC - Business User
SAP_GRC_FN_BUSINESS_USER	GRC - Business User
SAP_GRC_FN_DISPLAY	GRC - Display
SAP_GRC_FN_POST	Role with Post Authority Only

SAP GRC Work Centers

You can use Work Centers to provide a central access point for GRC 10.0. They can be organized based on what the customer has been licensed to operate.

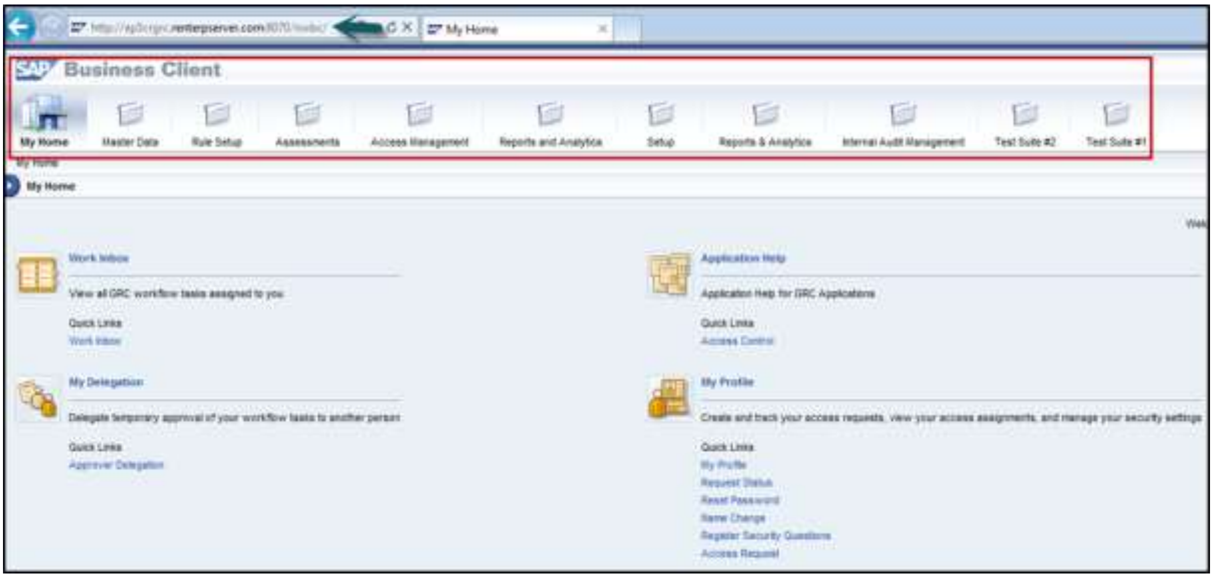
Step 1: To access Work Centers, open NetWeaver Business Client as mentioned above. Go to **/nwbc** option at the top to open Work Centers.



Launch NetWeaver Business Client

Cockpit nwbc	Content Lifecycle Management - GRC Access Control 10.0, Content Lifecycle Management - GRC Global Trade Services 10.0, Content Lifecycle Management - GRC Process Control 10.0 Role, Content Lifecycle Management - GRC Risk Managment 10.0 Role, Content Lifecycle Management - GRC 10.0 Role, GRC PFCG Authorization, ...
POA/CLM_GRC_AC_USER	Content Lifecycle Management - GRC Access Control 10.0
POA/CLM_GRC_GTS_USER	Content Lifecycle Management - GRC Global Trade Services 10.0
POA/CLM_GRC_PC_USER	Content Lifecycle Management - GRC Process Control 10.0 Role
POA/CLM_GRC_RM_USER	Content Lifecycle Management - GRC Risk Managment 10.0 Role
POA/CLM_GRC_USER	Content Lifecycle Management - GRC 10.0 Role
GRC_PFCG	GRC PFCG Authorization
SAP_DAL_ADMIN	Desktop Application Launcher Administration
SAP_DAL_ADMIN_DEALERPORTAL	Dealer Portal Admin Role for NWBC
SAP_DAL_ADMIN_MAINT_WORKER	EAMS role for NWBC path
SAP_DAL_ADMIN_PC	SAP_DAL_ADMIN_PC
SAP_DAL_ADMIN_SMI	Administrator Supplier-Managed Inventory
SAP_DAL_ADMIN_WORKFLOW_POWL	Business Workflow: Inbox Using POWL
SAP_DAL_DEMO_ROLE_1	SAP Desktop Application Launcher Demo Role #1
SAP_DAL_DEMO_ROLE_2	SAP Desktop Application Launcher Demo Role #2
SAP_GRC_FN_ADISSUE_PROCESS	Ad-hoc Issue Processer
SAP_GRC_FN_ALL	GRC - Power User
SAP_GRC_FN_ALL	GRC - Power User
SAP_GRC_FN_BASE	GRC - Base role to run GRC applications
SAP_GRC_FN_BASE	GRC - Base role to run GRC applications
SAP_GRC_FN_BUSINESS_USER	GRC - Business User
SAP_GRC_FN_BUSINESS_USER	GRC - Business User
SAP_GRC_FN_DISPLAY	GRC - Display
SAP_GRC_FN_POST	Role with Post Authority Only

Step 2: Once you click, you will be directed to the home screen of SAP NetWeaver Business client.



Work Inbox

View all GRC workflow tasks assigned to you

Quick Links
Work Inbox

Application Help

Application Help for GRC Applications

Quick Links
Access Control

My Delegation

Delegate temporary approval of your workflow tasks to another person

Quick Links
Approver Delegation

My Profile

Create and track your access requests, view your access assignments, and manage your security settings

Quick Links
My Profile
Request Status
Reset Password
Name Change
Register Security Questions
Access Request

Depending on the products that you have licensed, different components of the GRC solution are displayed: **Access Control, Process Control, or Risk Management**.

3. SAP GRC — Access Control

SAP GRC access control helps organizations to automatically detect, manage and prevent access risk violations and reduce unauthorized access to company data and information. Users can use automatic self-service to access request submission, workflow driven access request and approvals of access. Automatic reviews of user access, role authorization and risk violations can be used using SAP GRC Access Control.

SAP GRC Access Control handles key challenges by allowing business to manage access risk. It helps organizations to prevent unauthorized access by defining segregation of duties SoD and critical access and minimizing the time and cost of access risk management.

Key Features

The following are the key features of SAP GRC Access Control:

- To perform audit and compliance as per legal requirements with different audit standards like SOX, BSI and ISO standards.

- To automatically detect access risk violations across SAP and non-SAP systems in an organization.

- As mentioned, it empowers users with self-service access submission, workflow-driven access requests and approvals of the request.

- To automate reviews of user access, role authorizations, risk violations, and control assignments in a small and large scale organization.

- To efficiently manage the super-user access and avoiding risk violations and unauthorized access to data and application in SAP and non-SAP system.

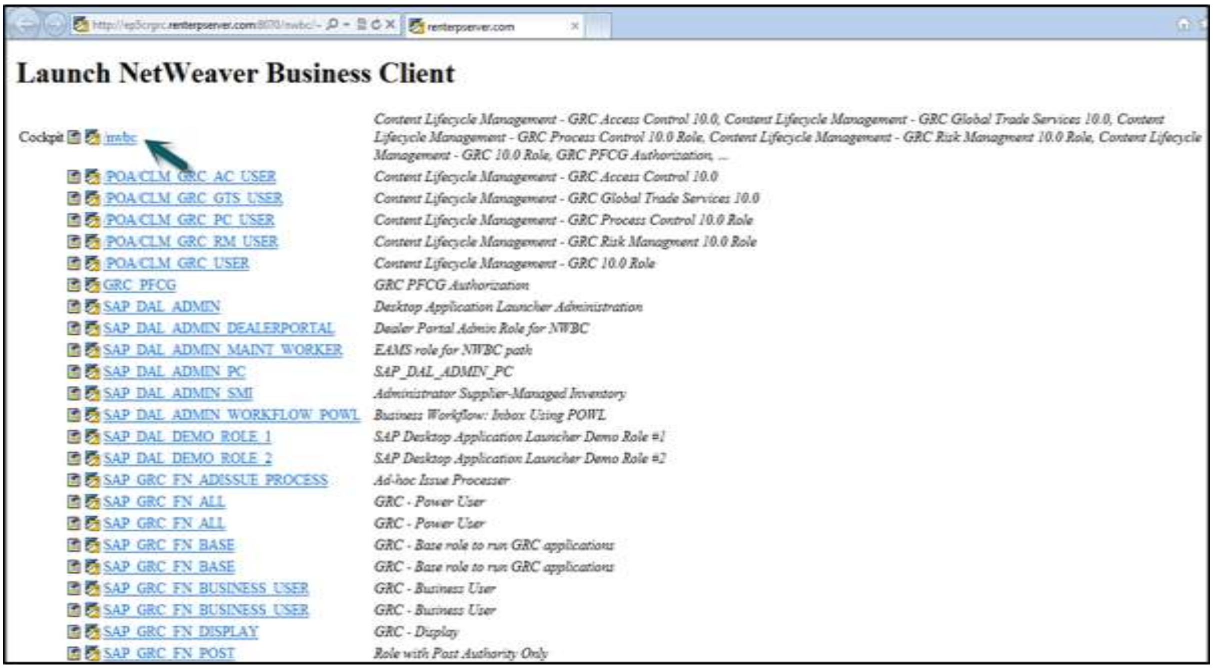
How to Explore Access Control Set Up Work Center?

Run the transaction for NWBC in SAP Easy access.

It will open NetWeaver Business Client screen and you will receive the following url:

http://ep5crgrc.renterpserver.com:8070/nwbc/~launch/?sap-client=800&sap-language=EN

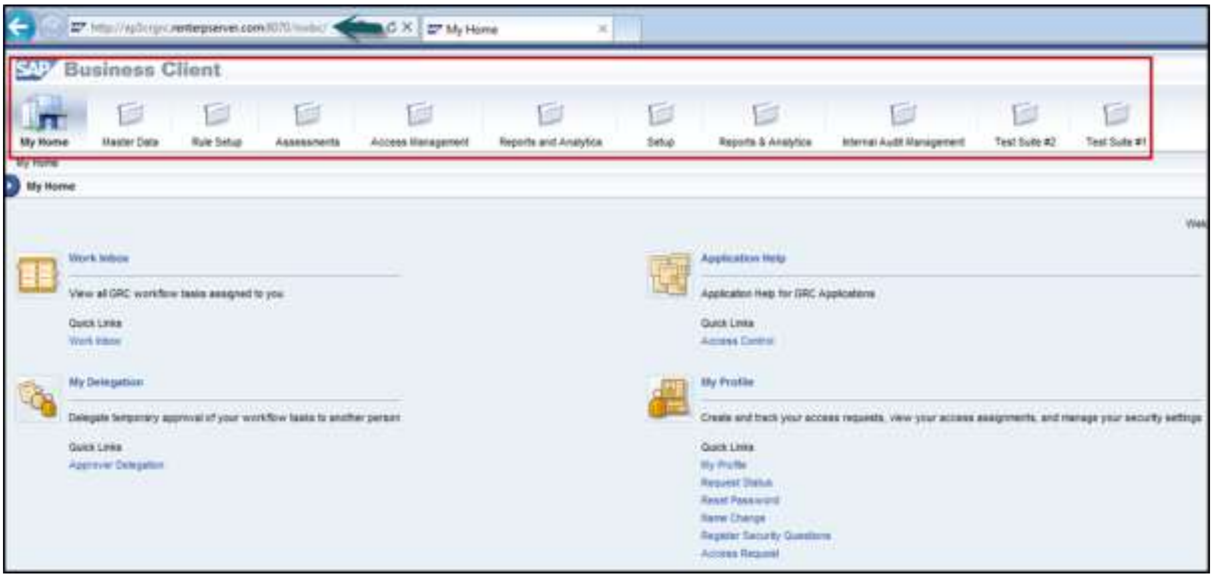
Step 1: To access Work Centers, open NetWeaver Business Client as mentioned above. Go to **/nwbc** option at the top to open Work Centers.



Launch NetWeaver Business Client

Cockpit nwbc	Content Lifecycle Management - GRC Access Control 10.0, Content Lifecycle Management - GRC Global Trade Services 10.0, Content Lifecycle Management - GRC Process Control 10.0 Role, Content Lifecycle Management - GRC Risk Managment 10.0 Role, Content Lifecycle Management - GRC 10.0 Role, GRC PFCG Authorization, ...
POA/CLM GRC AC USER	Content Lifecycle Management - GRC Access Control 10.0
POA/CLM GRC GTS USER	Content Lifecycle Management - GRC Global Trade Services 10.0
POA/CLM GRC PC USER	Content Lifecycle Management - GRC Process Control 10.0 Role
POA/CLM GRC RM USER	Content Lifecycle Management - GRC Risk Managment 10.0 Role
POA/CLM GRC USER	Content Lifecycle Management - GRC 10.0 Role
GRC PFCG	GRC PFCG Authorization
SAP DAL ADMIN	Desktop Application Launcher Administration
SAP DAL ADMIN DEALERPORTAL	Dealer Portal Admin Role for NWBC
SAP DAL ADMIN MAINT WORKER	EAMS role for NWBC path
SAP DAL ADMIN PC	SAP_DAL_ADMIN_PC
SAP DAL ADMIN SMI	Administrator Supplier-Managed Inventory
SAP DAL ADMIN WORKFLOW POWL	Business Workflow: Inbox Using POWL
SAP DAL DEMO ROLE 1	SAP Desktop Application Launcher Demo Role #1
SAP DAL DEMO ROLE 2	SAP Desktop Application Launcher Demo Role #2
SAP GRC FN ADISSUE PROCESS	Ad-hoc Issue Processer
SAP GRC FN ALL	GRC - Power User
SAP GRC FN ALL	GRC - Power User
SAP GRC FN BASE	GRC - Base role to run GRC applications
SAP GRC FN BASE	GRC - Base role to run GRC applications
SAP GRC FN BUSINESS USER	GRC - Business User
SAP GRC FN BUSINESS USER	GRC - Business User
SAP GRC FN DISPLAY	GRC - Display
SAP GRC FN POST	Role with Post Authority Only

Step 2: Once you click, you will be directed to the home screen of SAP NetWeaver Business client.



Work Inbox

View all GRC workflow tasks assigned to you

Quick Links

Work Inbox

My Delegation

Delegate temporary approval of your workflow tasks to another person

Quick Links

Approver Delegation

Application Help

Application Help for GRC Applications

Quick Links

Access Control

My Profile

Create and track your access requests, view your access assignments, and manage your security settings

Quick Links

My Profile

Request Status

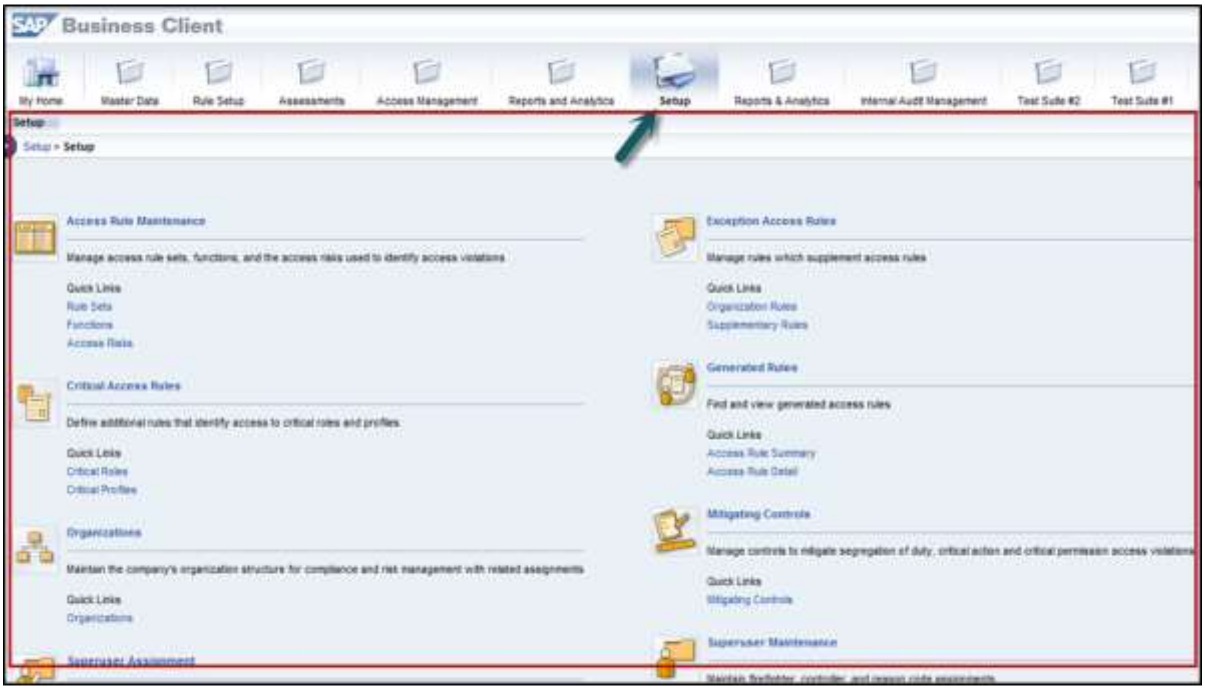
Reset Password

Name Change

Register Security Questions

Access Request

Step 3: Go to setup work center and explore the work set. Click some of the links under each one and explore the various screens.



Access Rule Maintenance

Manage access rule sets, functions, and the access risks used to identify access violations

Quick Links
Rule Sets
Functions
Access Risks

Exception Access Rules

Manage rules which supplement access rules

Quick Links
Organization Rules
Supplementary Rules

Critical Access Rules

Define additional rules that identify access to critical roles and profiles

Quick Links
Critical Roles
Critical Profiles

Generated Rules

Find and view generated access rules

Quick Links
Access Rule Summary
Access Rule Detail

Organizations

Maintain the company's organization structure for compliance and risk management with related assignments

Quick Links
Organizations

Mitigating Controls

Manage controls to mitigate segregation of duty, critical action and critical permission access violations

Quick Links
Mitigating Controls

Superuser Assignment

Superuser Maintenance

Maintain firefighter, controller, and reason code assignments

Step 4: The Setup work center is available in Access Control and provides links to the following sections:

- Access Rule Maintenance
- Exception Access Rules
- Critical Access Rules
- Generated Rules
- Organizations
- Mitigating Controls
- Superuser Assignment
- Superuser Maintenance
- Access Owners

Step 5: You can use the above listed functions in the following ways:

- Using Access Rule Maintenance section, you can manage access rule sets, functions, and the access risks used to identify access violations.
- Using Exception Access Rules, you can manage rules that supplement access rules.

- Using critical access rules section, you can define additional rules that identify access to critical roles and profiles.

- Using generated rules section, you can find and view generated access rules.

- Under Organizations, you can maintain the company's organization structure for compliance and risk management with related assignments.

- The Mitigating Controls section allows you to manage controls to mitigate segregation of duty, critical action, and critical permission access violations.

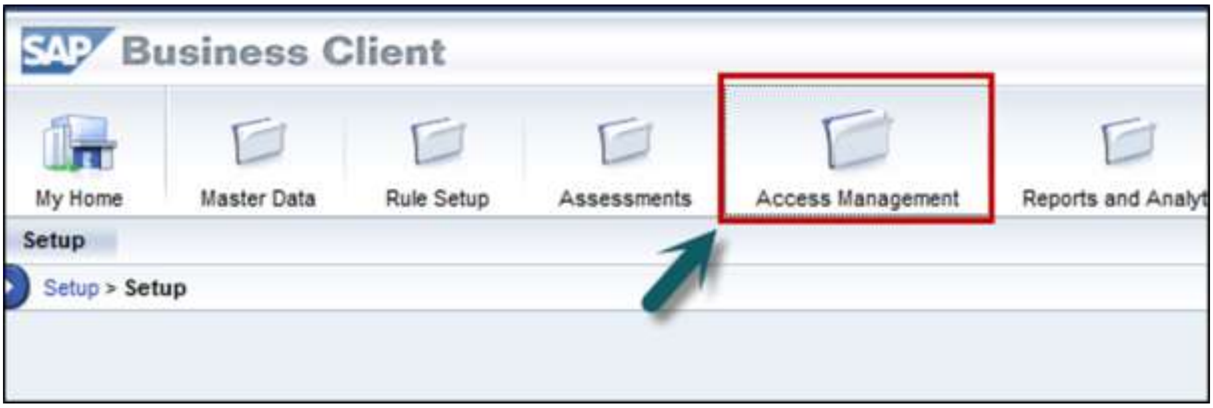
- Superuser Assignment is where you assign owners to firefighter IDs and assign firefighter IDs to users.

- Superuser Maintenance is where you maintain firefighter, controller, and reason code assignments.

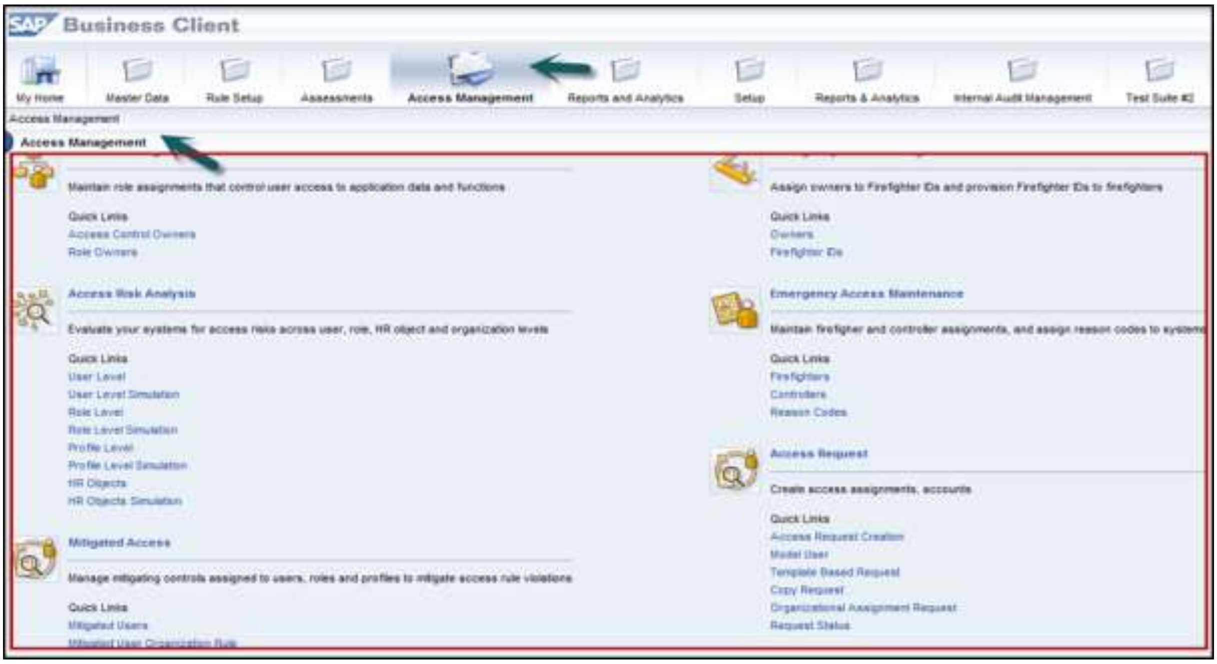
- Under Access Owners, you manage owner privileges for access management capabilities.

4. SAP GRC — Access Management Work Center

As per GRC software license, you can navigate Access Management Work Center. It has multiple sections to manage access control activities.



When you click on Access Management Work Center, you can see the following sections:



Maintain role assignments that control user access to application data and functions

Quick Links
Access Control Owners
Role Owners

Access Risk Analysis

Evaluate your systems for access risks across user, role, HR object and organization levels

Quick Links
User Level
User Level Simulation
Role Level
Role Level Simulation
Profile Level
Profile Level Simulation
HR Objects
HR Objects Simulation

Mitigated Access

Manage mitigating controls assigned to users, roles and profiles to mitigate access rule violations

Quick Links
Mitigated Users
Mitigated User Organization Rule

Assign owners to Firefighter IDs and provision Firefighter IDs to firefighters

Quick Links
Owners
Firefighter IDs

Emergency Access Maintenance

Maintain firefighter and controller assignments, and assign reason codes to system

Quick Links
Firefighters
Controllers
Reason Codes

Access Request

Create access assignments, accounts

Quick Links
Access Request Creation
Model User
Template Based Request
Copy Request
Organizational Assignment Request
Request Status

- GRC Role Assignments
- Access Risk Analysis
- Mitigated Access
- Access Requests Administration
- Role Management

- Role Mining
- Role Mass Maintenance
- Superuser Assignment
- Superuser Maintenance
- Access Request Creation
- Compliance Certification Reviews
- Alerts
- Scheduling

The above sections help you in the following ways:

- When you go to access **risk analysis** section, you can evaluate your systems for access risks across users, roles, HR objects and organization levels. An access risk is two or more actions or permissions that, when available to a single user or single role, profile, organizational level, or HR Object, creates the possibility of error or irregularity.

- Using **mitigated access** section, you can identify access risks, assess the level of those risks, and assign mitigating controls to users, roles, and profiles to mitigate the access rule violations.

- In **access request administration** section, you can manage access assignments, accounts, and review processes.

- Using **role management**, you manage roles from multiple systems in a single unified repository.

- In **role mining** group feature, you can target roles of interest, analyze them, and take action.

- Using **role mass maintenance**, you can import and change authorizations and attributes for multiple roles.

- In **Superuser Assignment** section, you can assign firefighter IDs to owners and assign firefighters and controllers to firefighter IDs.

- In **Superuser Maintenance** section, you can perform activities such as researching and maintaining firefighters and controllers, and assigning reason codes by system.

- Using **access request creation**, you can create access assignments and accounts.

- **Compliance certification reviews** supports reviews of users' access, risk violations and role assignments.

- Using **alerts**, you can generate by the application for execution of critical or conflicting actions.

- Using **Scheduling** section of the Rule Setup Work Center, you can maintain schedules for continuous control monitoring and automated testing, and to track related job progress.

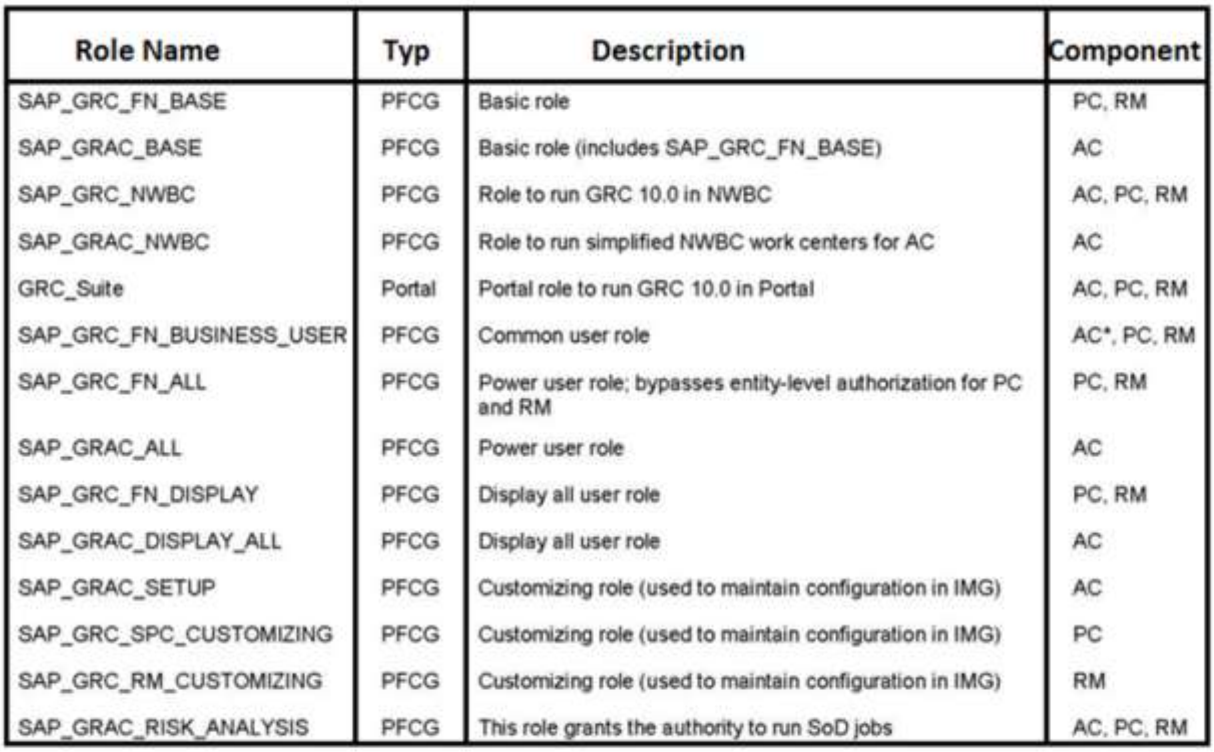
5. SAP GRC — Access & Authorization Management

In SAP GRC solution, you can manage authorization objects to limit the items and data that a user can access. Authorization controls what a user can access in regards to work centers and reports in SAP system.

To access GRC solution, you should have following access:

- Portal authorization
- Applicable PFCG roles
- PFCG roles for access control, process control and risk management

The authorization types listed below are required as per GRC components: AC, PC and RM.

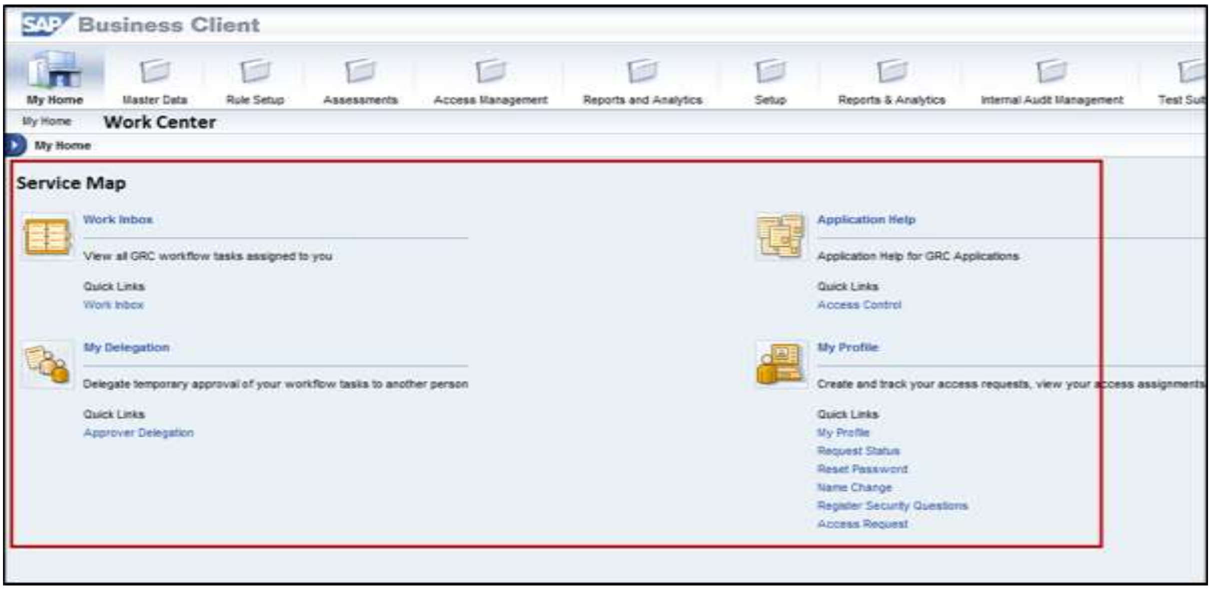


Role Name	Typ	Description	Component
SAP_GRC_FN_BASE	PFCG	Basic role	PC, RM
SAP_GRAC_BASE	PFCG	Basic role (includes SAP_GRC_FN_BASE)	AC
SAP_GRC_NWBC	PFCG	Role to run GRC 10.0 in NWBC	AC, PC, RM
SAP_GRAC_NWBC	PFCG	Role to run simplified NWBC work centers for AC	AC
GRC_Suite	Portal	Portal role to run GRC 10.0 in Portal	AC, PC, RM
SAP_GRC_FN_BUSINESS_USER	PFCG	Common user role	AC*, PC, RM
SAP_GRC_FN_ALL	PFCG	Power user role; bypasses entity-level authorization for PC and RM	PC, RM
SAP_GRAC_ALL	PFCG	Power user role	AC
SAP_GRC_FN_DISPLAY	PFCG	Display all user role	PC, RM
SAP_GRAC_DISPLAY_ALL	PFCG	Display all user role	AC
SAP_GRAC_SETUP	PFCG	Customizing role (used to maintain configuration in IMG)	AC
SAP_GRC_SPC_CUSTOMIZING	PFCG	Customizing role (used to maintain configuration in IMG)	PC
SAP_GRC_RM_CUSTOMIZING	PFCG	Customizing role (used to maintain configuration in IMG)	RM
SAP_GRAC_RISK_ANALYSIS	PFCG	This role grants the authority to run SoD jobs	AC, PC, RM

Authorization in Portal Component and NWBC

In SAP GRC 10.0 solution, work centers are defined in PCD roles for the Portal component and in PFCG roles for NWBC (**NetWeaver Business Client)**. The work centers are fixed in each base role. SAP delivers these roles however; these roles can be modified by the customer as per requirement.

The locations of application folders and subordinate applications within the service map are controlled by the SAP NetWeaver Launchpad application. Service map is controlled by user authorization so if user doesn't have authorization to see any application they will be hidden in NetWeaver Business client.



View all GRC workflow tasks assigned to you

Delegate temporary approval of your workflow tasks to another person

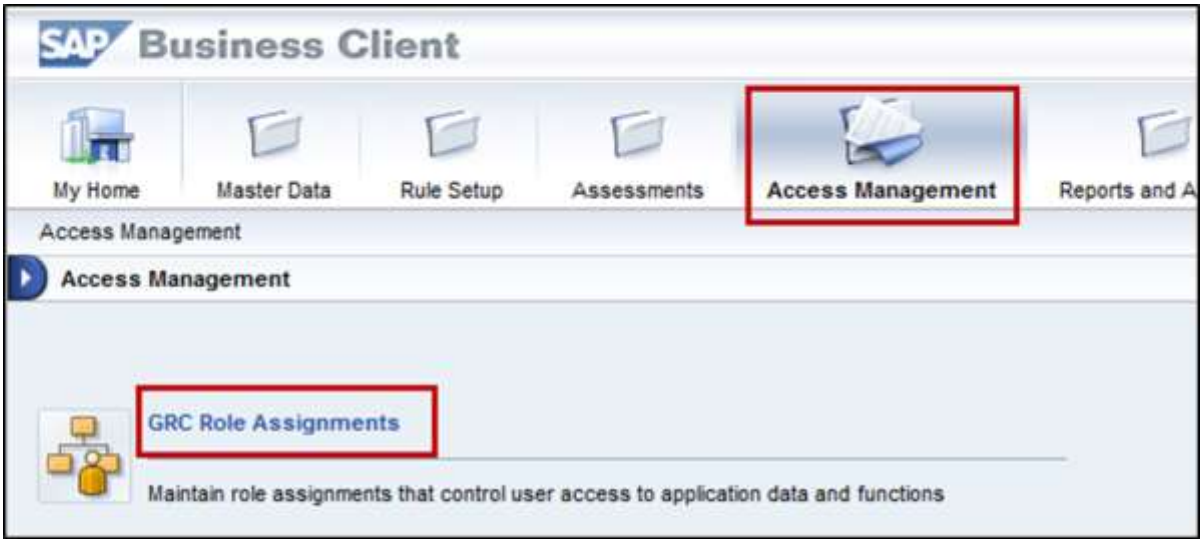
Application Help for GRC Applications

Create and track your access requests, view your access assignments

How to review role assignments in Access Management Work Center?

Follow these steps to review role assignments:

Step 1: Go to Access Management Work Center in NetWeaver Business Client.

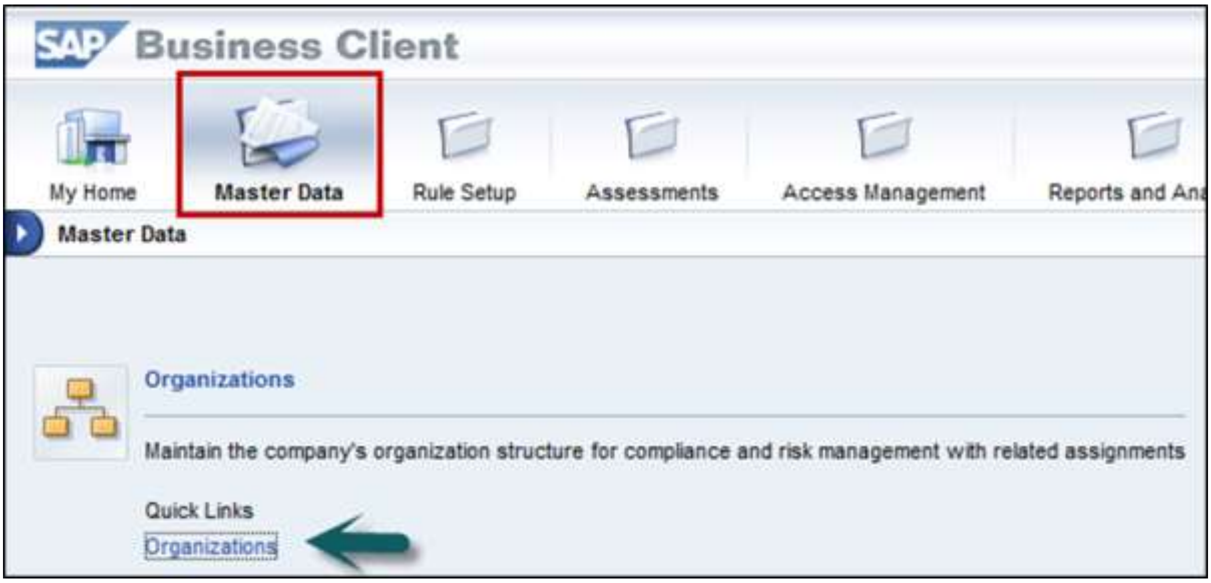


Maintain role assignments that control user access to application data and functions

Step 2: Select business process under GRC Role assignment and go to sub-process role level. Click next to continue to assign role sections.

How to review role assignments in the Master Data Work Center?

Step 1: Go to Master Data Work Center -> Organizations



Master Data

Organizations

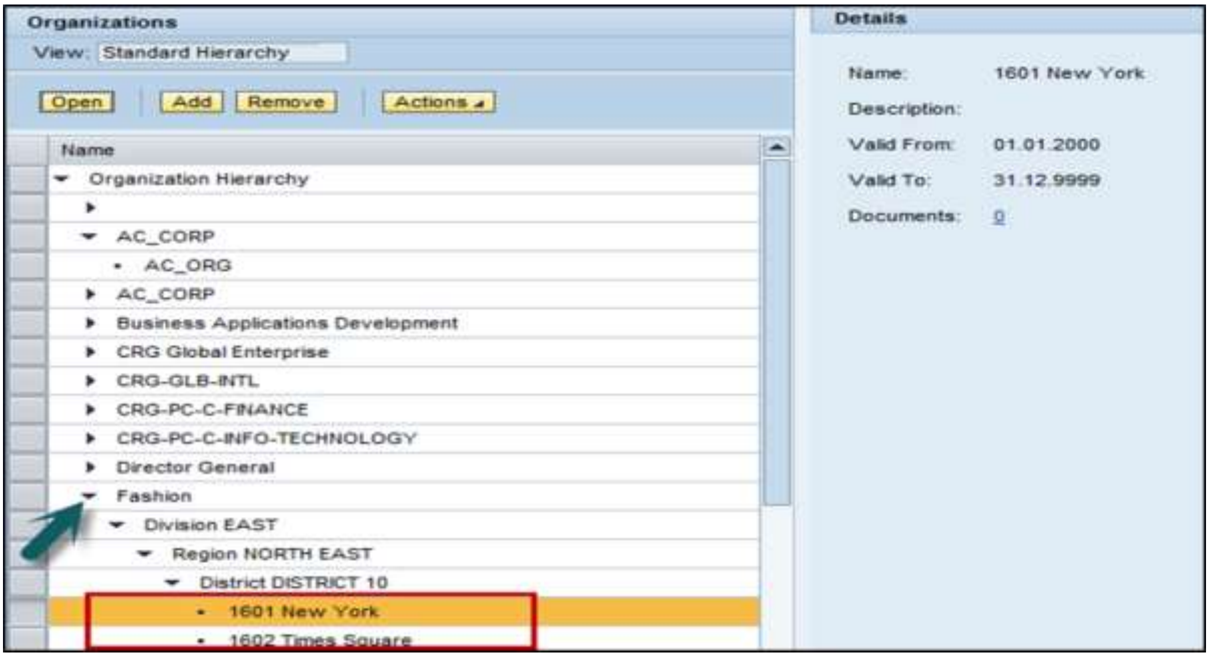
Maintain the company's organization structure for compliance and risk management with related assignments

Quick Links

Organizations

Step 2: In next window, select any organization from the list, then click Open.

Step 3: Note that the triangle next to the organization means that there are sub-organizations and the dot next to the organization means that it is the lowest level.



View: Standard Hierarchy

Name
- Organization Hierarchy
  -
  - AC_CORP
    - AC_ORG
  - AC_CORP
  - Business Applications Development
  - CRG Global Enterprise
  - CRG-GLB-INTL
  - CRG-PC-C-FINANCE
  - CRG-PC-C-INFO-TECHNOLOGY
  - Director General
  - Fashion
    - Division EAST
      - Region NORTH EAST
        - District DISTRICT 10
          - 1601 New York
          - 1602 Times Square

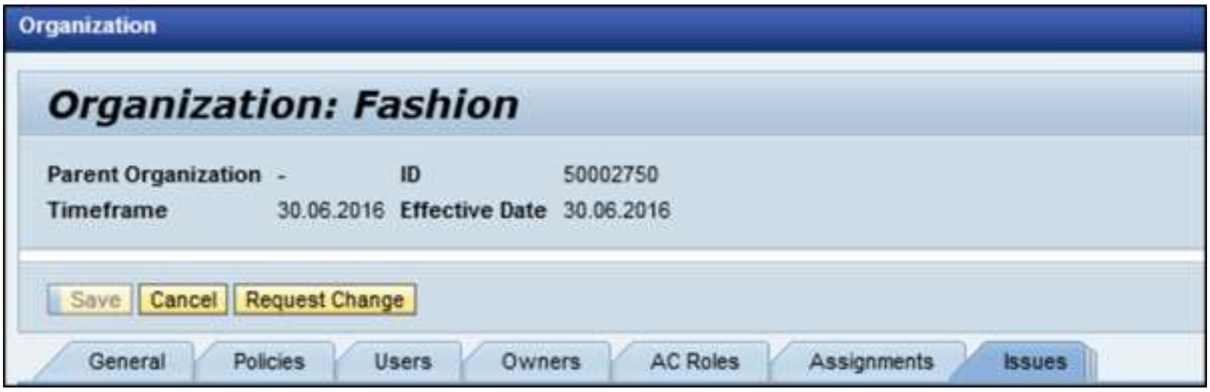
Name:	1601 New York
Description:	
Valid From:	01.01.2000
Valid To:	31.12.9999
Documents:	0

Step 4: Click on subprocess tab -> Assign subprocess. Now select one or two subprocesses and click on Next.

Step 5: Without making any changes, click Finish on the Select Controls step.

Step 6: Choose the first subprocess from the list, then click Open. You should see the subprocess details.

Step 7: Click the Roles Tab. Choose a role from the list, then click Assign.



Organization

Organization: Fashion

Parent Organization - ID 50002750

Timeframe 30.06.2016 Effective Date 30.06.2016

6. SAP GRC — Authorization

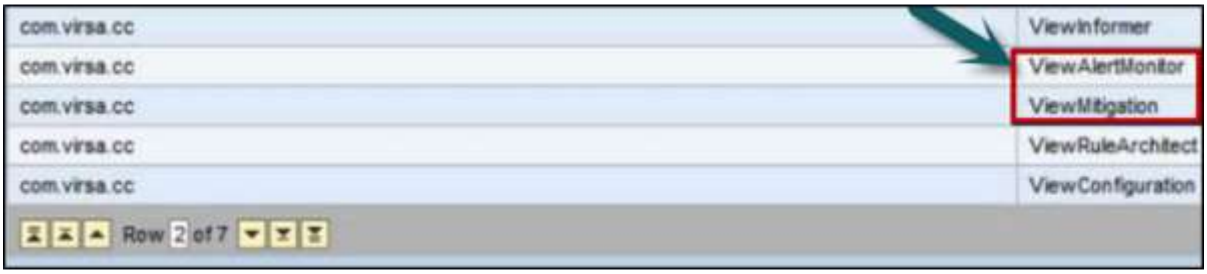
SAP GRC Access Control uses UME roles to control the user authorization in the system. An administrator can use actions which represent the smallest entity of UME role that a user can use to build access rights.

One UME role can contain actions from one or more applications. You have to assign UME roles to users in **User Management Engine (UME)**.

Authorization in UME

When a user does not have access to a certain tab, the tab will not display upon user logon when the user tries to access that tab. When a UME action for a tab is assigned to that particular user, only then he will be able to access that function.

All available standard UME actions for CC tabs can be found in the tab **"Assigned Actions"** of the **Admin User**.



com.virsa.cc	ViewInformer
com.virsa.cc	ViewAlertMonitor
com.virsa.cc	ViewMitigation
com.virsa.cc	ViewRuleArchitect
com.virsa.cc	ViewConfiguration

UME Roles

You should create an administrator role and this role should be assigned to Superuser to perform SAP compliance calibrator related activities. There are various CC roles that can be created under SAP GRC Access control at the time of implementation:

- **CC.ReportingView**
  Description: Compliance Calibrator Display and Reporting

- **CC.RuleMaintenance**
  Description: Compliance Calibrator Rule Maintenance

- **CC.MitMaintenance**
  Description: Compliance Calibrator Mitigation Maintenance

- **CC.Administration**
  Description: Compliance Calibrator Administration and Basis Configuration

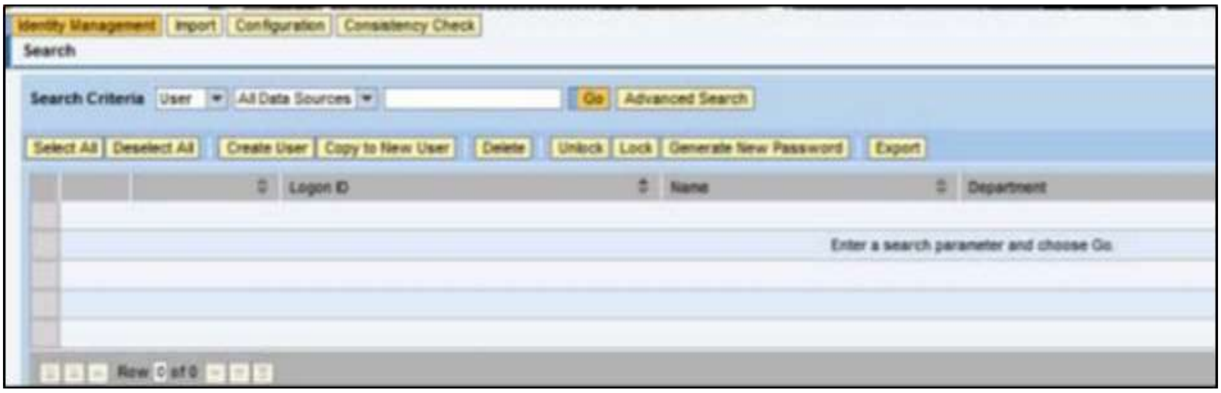
How to open User Maintenance Engine?

Using UME, you can perform various key activities under Access Control:

- You can perform user and role maintenance
- It can be used for user data source configuration
- You can apply security settings and password rules

To open UME, you should use the following URL:

http://<hostname>:<port>/useradmin



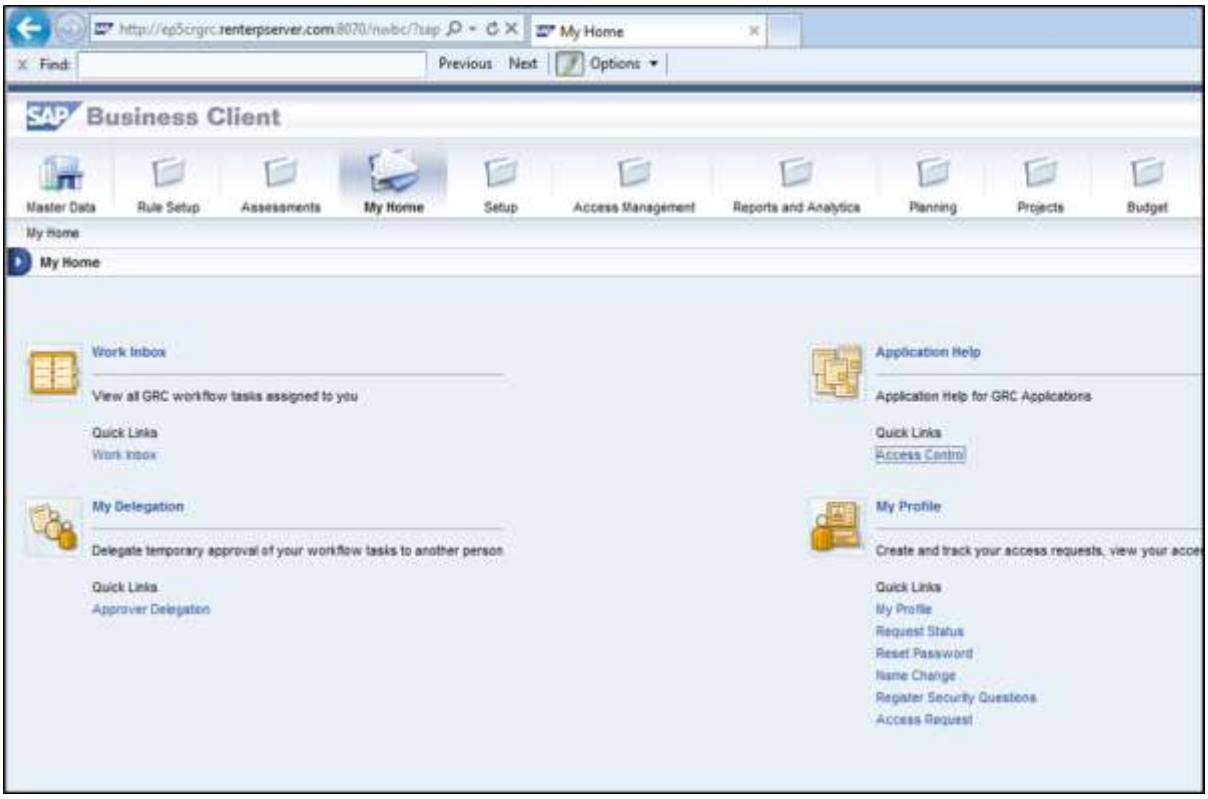
Enter a search parameter and choose Go.

7. SAP GRC — Access Control Launchpad

In SAP GRC 10.0, you can use Access Control Launch Pad to maintain key functionalities under GRC Access Control. It is a single web page that can be used for **Risk Analysis and Remediation (RAR)**.

In GRC Access Control, you can use Risk Analysis and Remediation (RAR) capability to perform security audit and segregation of duties (SoD) analysis. It is a tool which can be used to identify, analyze, and resolve risk and audit issues linked to the following regulatory compliance. Here, you can also colloaboratively define the following:

- Enterprise Role Management (ERM)
- Compliant User Provisioning (CUP)
- Superuser Privilege Management



Work Inbox

View all GRC workflow tasks assigned to you

Quick Links
Work Inbox

Application Help

Application Help for GRC Applications

Quick Links
Access Control

My Delegation

Delegate temporary approval of your workflow tasks to another person

Quick Links
Approver Delegation

My Profile

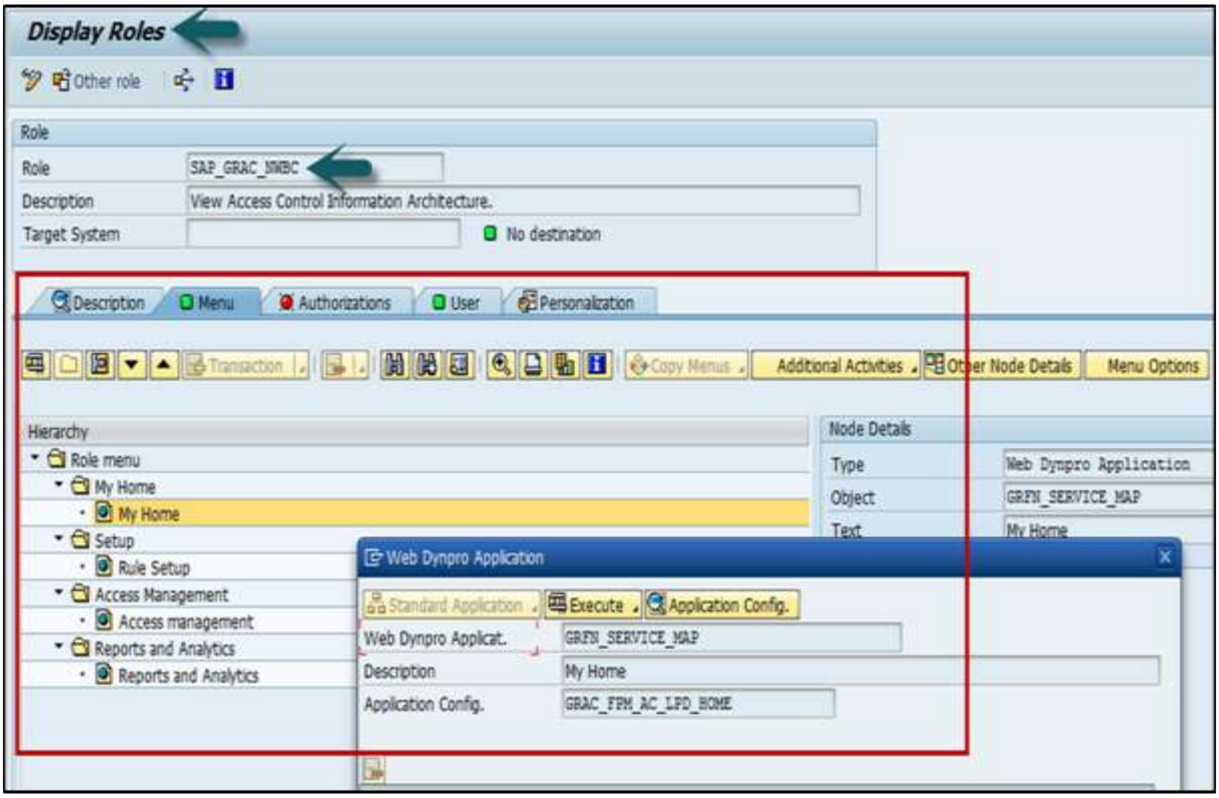
Create and track your access requests, view your acce

Quick Links
My Profile
Request Status
Reset Password
Name Change
Register Security Questions
Access Request

Creating a New Launchpad in NWBC

Follow these steps to create a new Launchpad in NWBC:

Step 1: Go to PFCG roles, and open the role SAP_GRAC_NWBC



Role

Role: SAP_GRAC_NWBC

Description: View Access Control Information Architecture.

Target System: No destination

Type: Web Dynpro Application

Object: GRFN_SERVICE_MAP

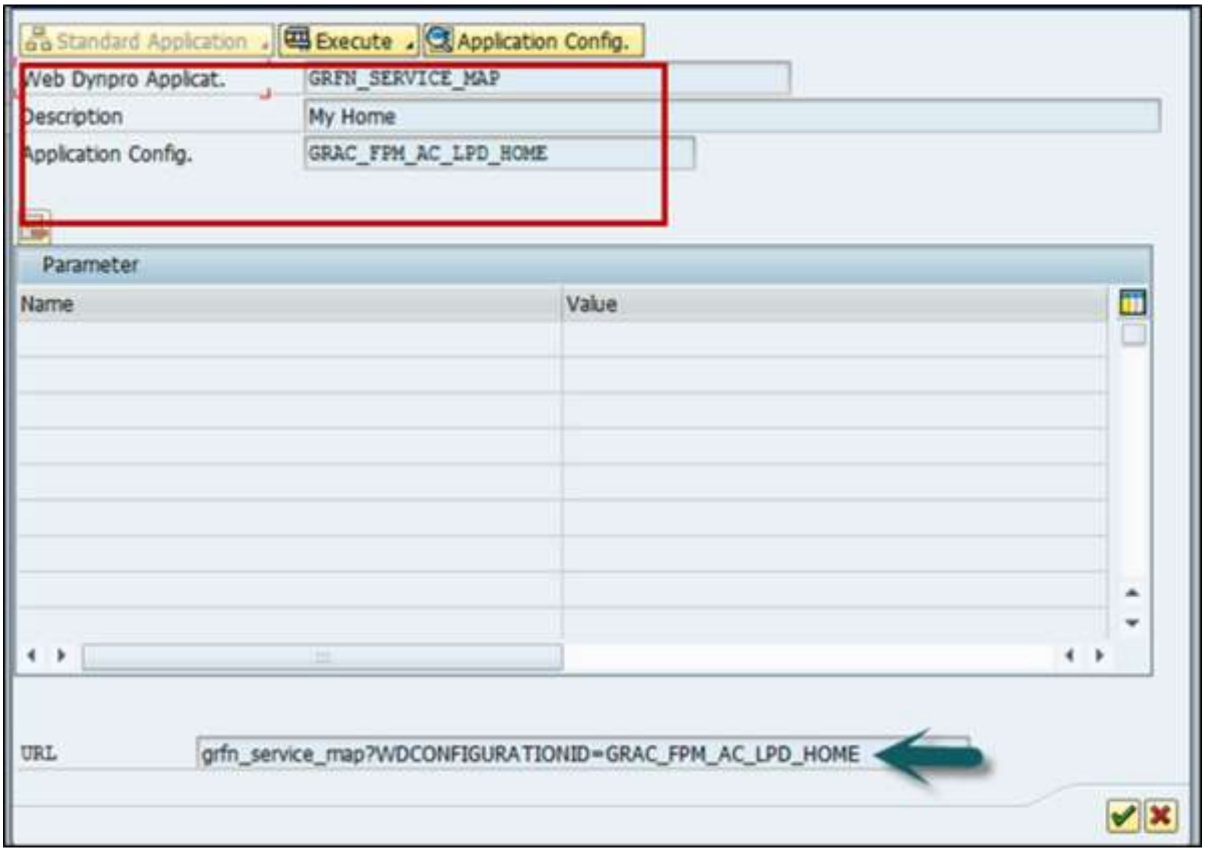
Text: My Home

Web Dynpro Applicat.: GRFN_SERVICE_MAP

Description: My Home

Application Config.: GRAC_FPM_AC_LPD_HOME

Step 2: When you right click **My Home** item, you can see the application being called is **grfn_service_map?WDCONFIGURATIONID=GRAC_FPM_AC_LPD_HOME** and the configuration id is **GRAC_FPM_AC_LPD_HOME**.



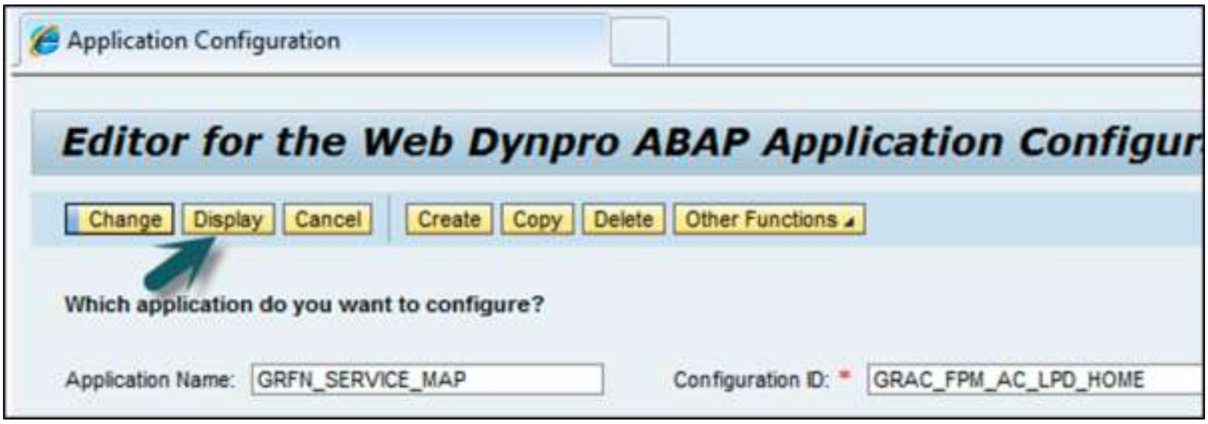
Web Dynpro Applicat. GRFN_SERVICE_MAP

Description My Home

Application Config. GRAC_FPM_AC_LPD_HOME

URL grfn_service_map?WDCONFIGURATIONID=GRAC_FPM_AC_LPD_HOME

Step 3: Select **application config** button and you can see the application configuration screen -> display button.



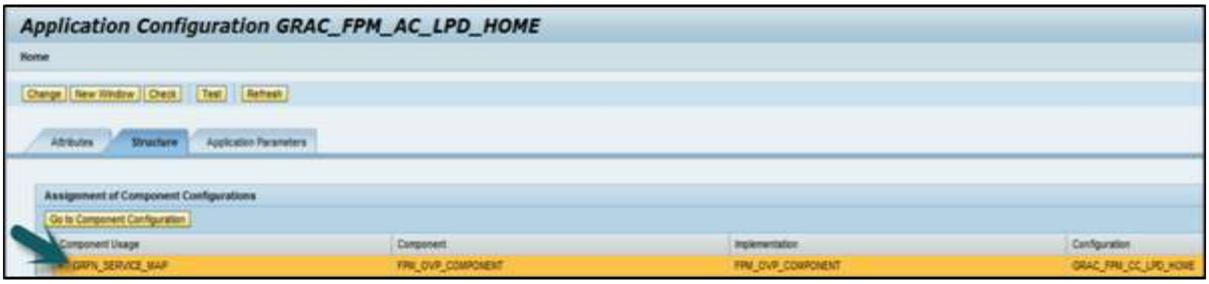
Editor for the Web Dynpro ABAP Application Configur

Which application do you want to configure?

Application Name: GRFN_SERVICE_MAP

Configuration ID: * GRAC_FPM_AC_LPD_HOME

Step 4: When you click on **Display**, you can see this screen:



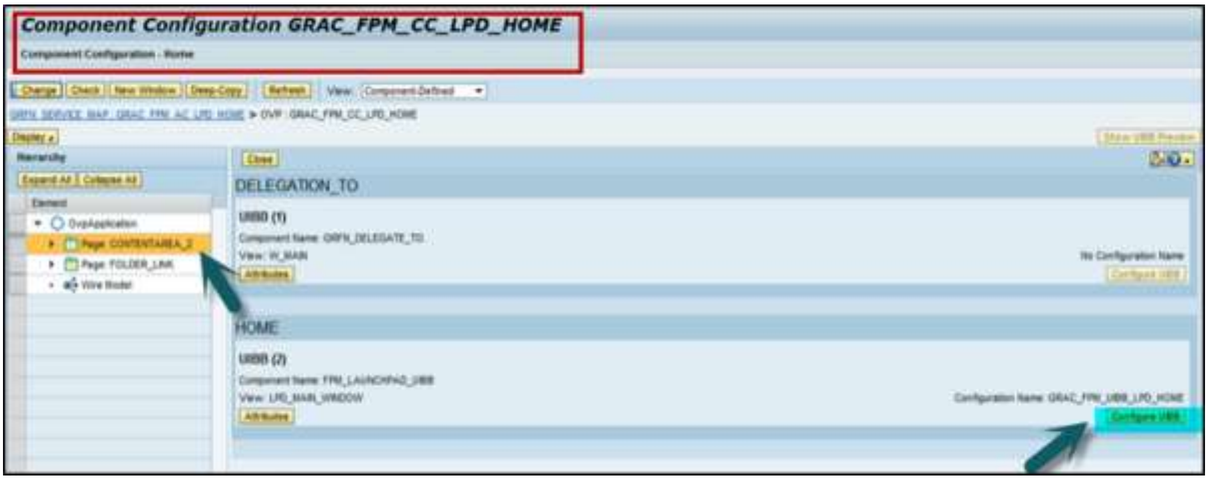
Application Configuration GRAC_FPM_AC_LPD_HOME

Home

Assignment of Component Configurations

Component Usage	Component	Implementation	Configuration
GRFN_SERVICE_MAP	FPM_OVP_COMPONENT	FPM_OVP_COMPONENT	GRAC_FPM_CC_LPD_HOME

Step 5: Now open the **Component Configuration** button.



Component Configuration GRAC_FPM_CC_LPD_HOME

Component Configuration - Home

View: Component-Defined

GRFN_SERVICE_MAP: GRAC_FPM_AC_LPD_HOME > OVP : GRAC_FPM_CC_LPD_HOME

Hierarchy

Element
- OvpApplication
  - Page: CONTENTAREA_2
  - Page: FOLDER_LINK
  - Wire Model

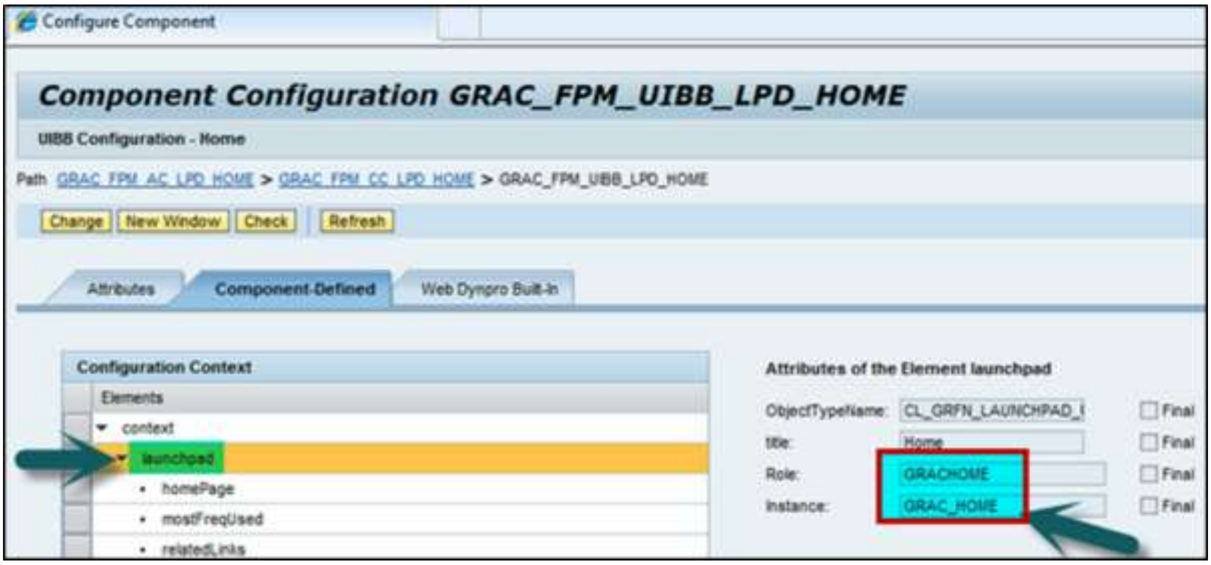
DELEGATION_TO

UIBB (1)
Component Name: GRFN_DELEGATE_TO
View: W_MAIN
No Configuration Name

HOME

UIBB (2)
Component Name: FPM_LAUNCHPAD_UIBB
View: LPD_MAIN_WINDOW
Configuration Name: GRAC_FPM_UIBB_LPD_HOME

Step 6: Click on **Configure UIBB** button in this screen. You will be directed to the following screen:



Component Configuration GRAC_FPM_UIBB_LPD_HOME

UIBB Configuration - Home

Path GRAC_FPM_AC_LPD_HOME > GRAC_FPM_CC_LPD_HOME > GRAC_FPM_UIBB_LPD_HOME

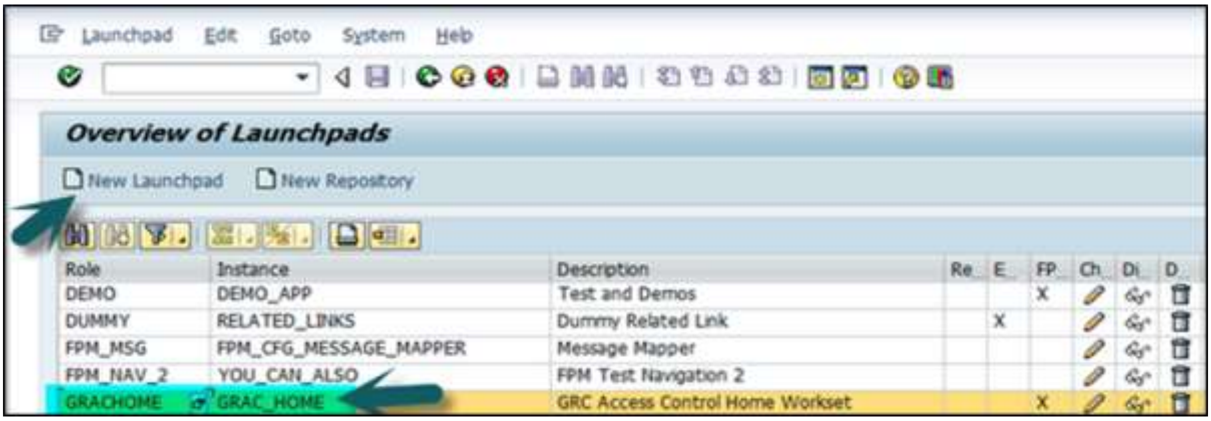
Configuration Context

Elements
- context
  - launchpad
    - homePage
    - mostFreqUsed
    - relatedLinks

Attributes of the Element launchpad

ObjectTypeName:	CL_GRFN_LAUNCHPAD_I	□ Final
title:	Home	□ Final
Role:	GRACHOME	□ Final
Instance:	GRAC_HOME	□ Final

Step 7: You can select the Launchpad to which you want to map. If you want to create a new Launchpad, you can also map it to a new role.



Overview of Launchpads

Role	Instance	Description	Re	E	FP	Ch	Di	D
DEMO	DEMO_APP	Test and Demos			X			
DUMMY	RELATED_LINKS	Dummy Related Link		X				
FPM_MSG	FPM_CFG_MESSAGE_MAPPER	Message Mapper						
FPM_NAV_2	YOU_CAN_ALSO	FPM Test Navigation 2						
GRACHOME	GRAC_HOME	GRC Access Control Home Workset			X			

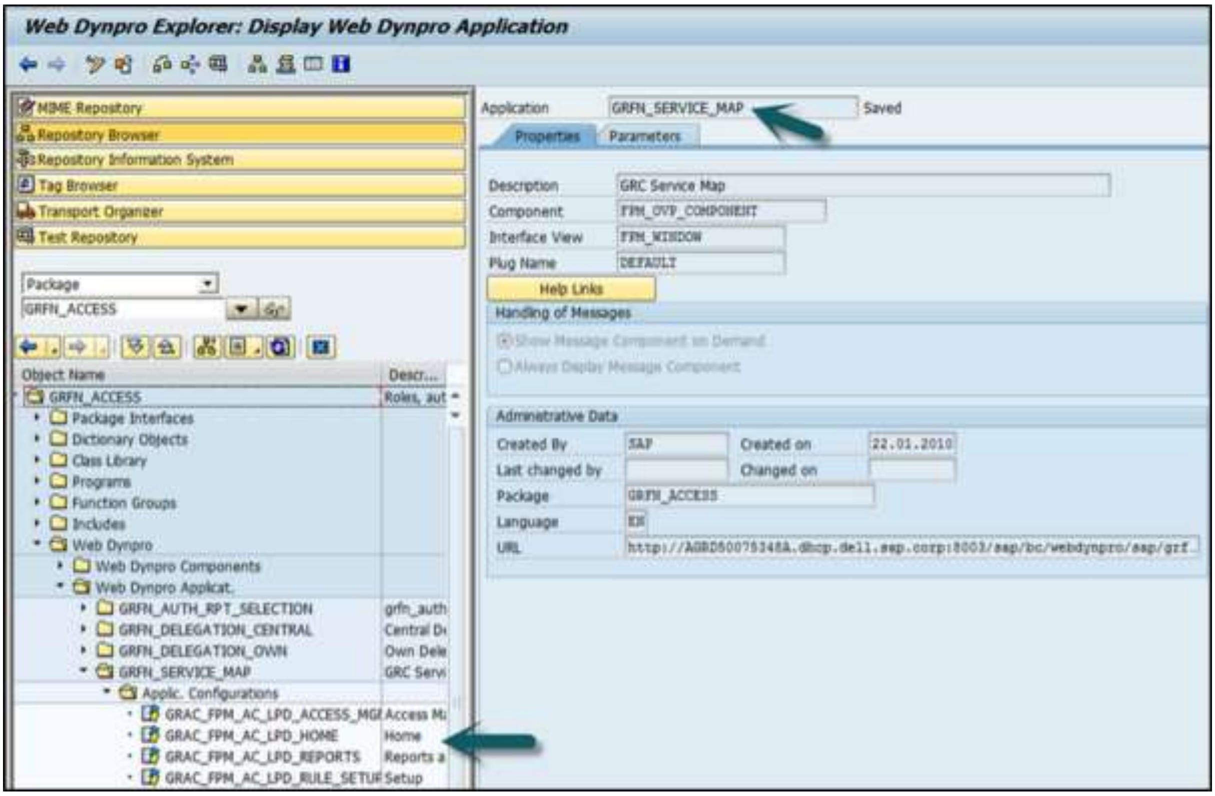
Step 8: To create a new Launchpad, define the following:

- Create a new launchpad with menu items that you want.

- Create a new configuration of the application **GRFN_SERVICE_MAP** or you can copy configuration id **GRAC_FPM_AC_LPD_HOME** and customize it further.

- In the new configuration select the launchpad that you want to associate.

- Create a new role and add webdynpro application **GRFN_SERVICE_MAP** to it with the custom configuration id created in the previous step.



Web Dynpro Explorer: Display Web Dynpro Application

Application: GRFN_SERVICE_MAP Saved

Description: GRC Service Map
Component: FPM_OVP_COMPONENT
Interface View: FPM_WINDOW
Plug Name: DEFAULT

Handing of Messages
● Show Message Component on Demand
○ Always Display Message Component

Administrative Data
Created By: SAP   Created on: 22.01.2010
Last changed by: Changed on:
Package: GRFN_ACCESS
Language: EN
URL: http://AGRD50075348A.dhcp.dell.sap.corp:8003/sap/bc/webdynpro/sap/grf

8. SAP GRC — Integration with Access Control

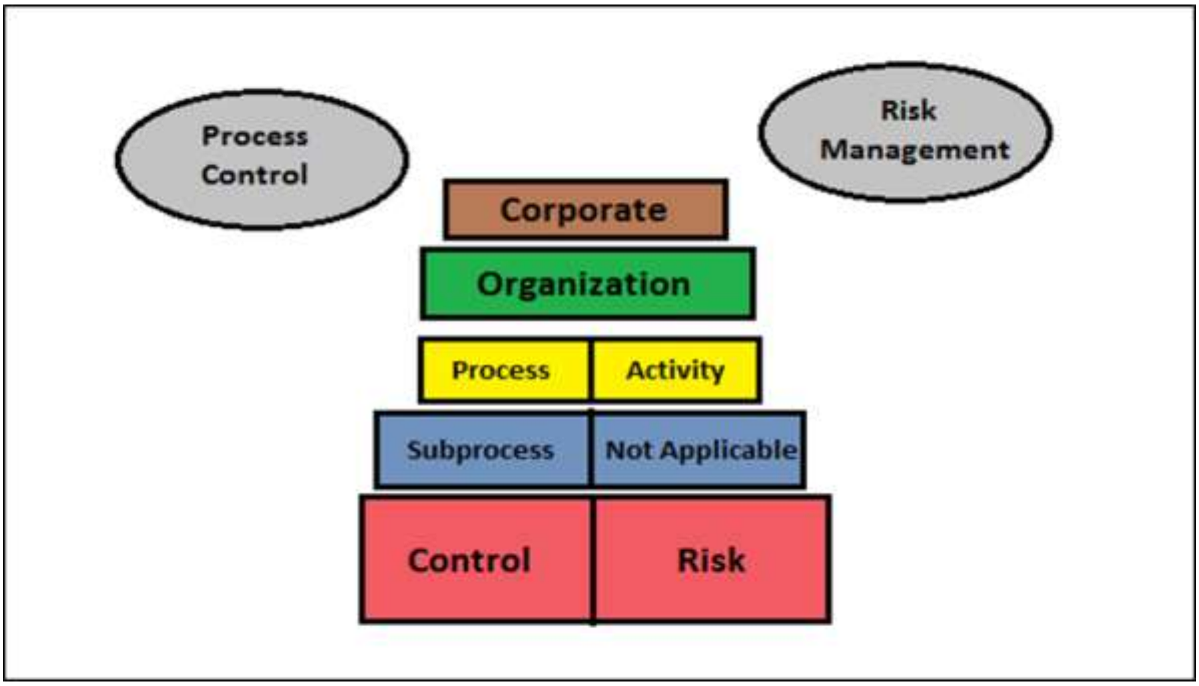
In SAP GRC 10.0 solution, the master data and organization structure is shared across access control, process control and risk management. Process Control also shares certain capabilities with risk management process.

Following are the key features shared with Access Control:

- Access control and process control shares the compliance structure in below areas:
  - In process control solution, controls are used as mitigation control in access control under SAP GRC 10.0 solution.
  - Access control and process control share same organization.
  - In process control, processes are used as business processes in access control.
  - Process control and access control are integrated with access risk analysis to monitor segregation of duties SoD.

The menu areas common to both Process Control and Risk Management are:

- GRC Role Assignment
- Process Control Planner
- Risk Management Planner
- Central Delegation



The following are the key integration points between Process Control and Risk Management:

- New control points can be purposed for Process Control in Risk Management.

- When a new control is proposed, Process Control needs to evaluate the request from Risk Management.

- Risk Management uses results from Process Control to evaluate new controls.

- Risk Management can also use existing controls from Process Control as responses in Risk Management.

9. SAP GRC — Integration with IAM

Internal Audit Management allows you to process the information from Risk Management and Process Control to use in audit planning. Audit proposal can be transferred to audit management for processing when required and audit items can be used to generate issues for reporting. IAM provides you a place where you can perform complete audit planning, create audit items, define audit universe and create and view audit reports and audit issues.

Internal Audit Management Work Center provides a central location for the following activities:

- Define the audit universe for your organization
- Audit risk rating
- Audit planning to define procedure for audit compliance
- Audit issues from audit actions
- Audit reports to see what risks are there on auditable entities

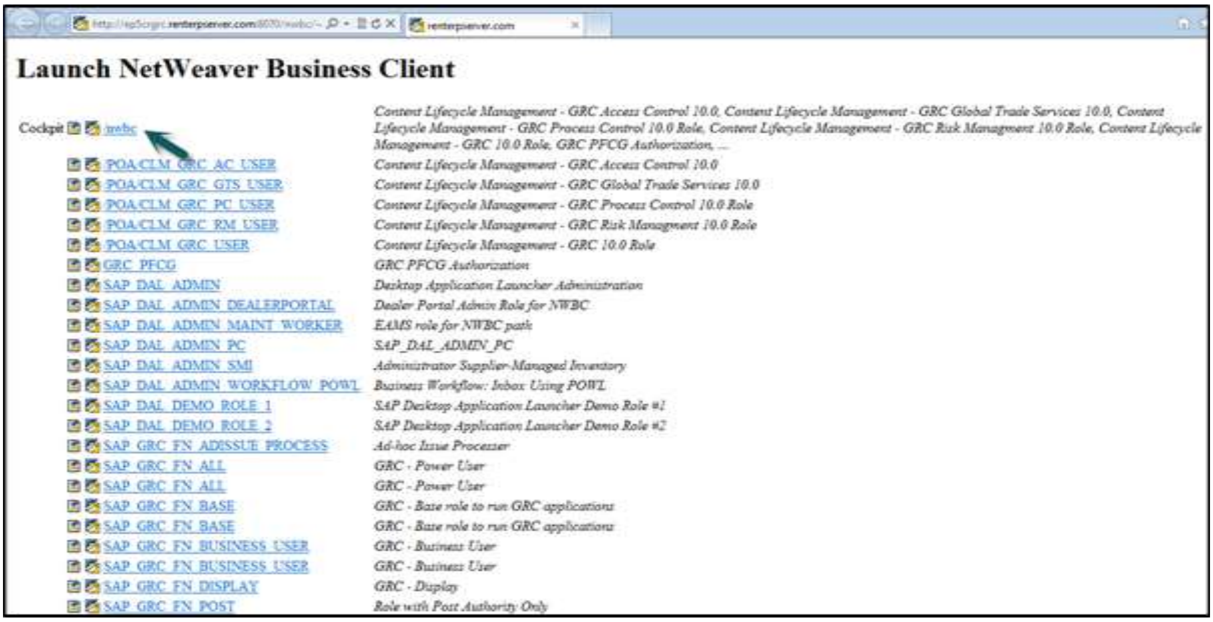
10. SAP GRC — Audit Universe

Audit Universe contains audit entities which can be classified as business units, lines of business or departments. Audit entities define the audit planning strategy and these can be linked to Process Control and Risk Management to find risks, controls, etc.

Create an Auditable Entity

Let us now understand how to create an auditable enity.

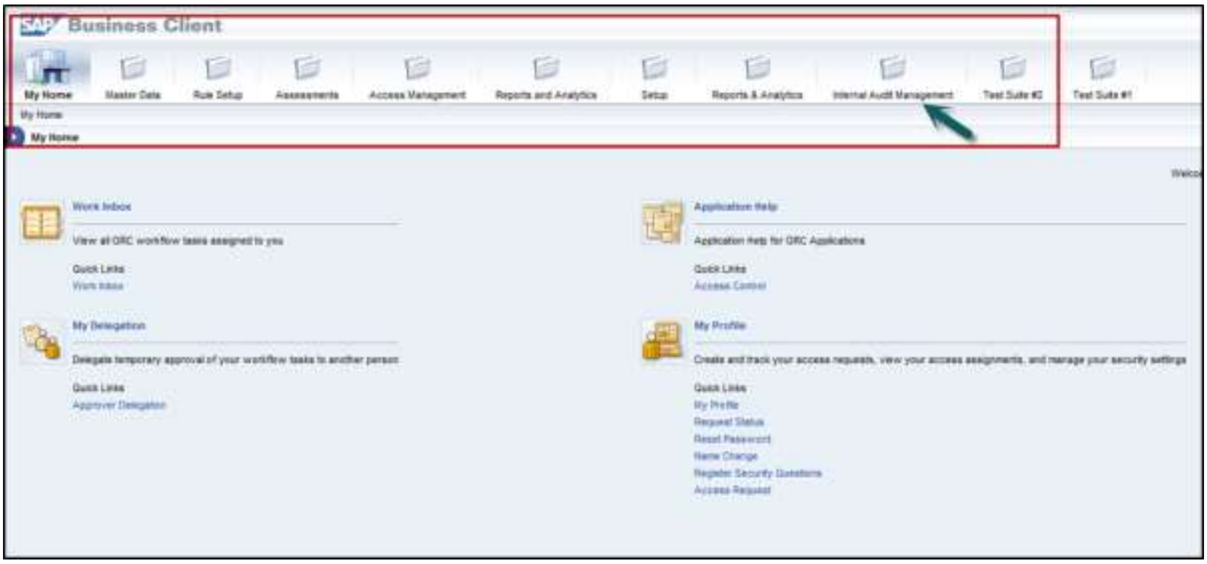
Step 1: Go to **/nwbc** option at the top to open Work Centers



Launch NetWeaver Business Client

Cockpit /nwbc	*Content Lifecycle Management - GRC Access Control 10.0, Content Lifecycle Management - GRC Global Trade Services 10.0, Content Lifecycle Management - GRC Process Control 10.0 Role, Content Lifecycle Management - GRC Risk Managment 10.0 Role, Content Lifecycle Management - GRC 10.0 Role, GRC PFCG Authorization, ...*
POA/CLM_GRC_AC_USER	*Content Lifecycle Management - GRC Access Control 10.0*
POA/CLM_GRC_GTS_USER	*Content Lifecycle Management - GRC Global Trade Services 10.0*
POA/CLM_GRC_PC_USER	*Content Lifecycle Management - GRC Process Control 10.0 Role*
POA/CLM_GRC_RM_USER	*Content Lifecycle Management - GRC Risk Managment 10.0 Role*
POA/CLM_GRC_USER	*Content Lifecycle Management - GRC 10.0 Role*
GRC_PFCG	*GRC PFCG Authorization*
SAP_DAL_ADMIN	*Desktop Application Launcher Administration*
SAP_DAL_ADMIN_DEALERPORTAL	*Dealer Portal Admin Role for NWBC*
SAP_DAL_ADMIN_MAINT_WORKER	*EAMS role for NWBC path*
SAP_DAL_ADMIN_PC	*SAP_DAL_ADMIN_PC*
SAP_DAL_ADMIN_SMI	*Administrator Supplier-Managed Inventory*
SAP_DAL_ADMIN_WORKFLOW_POWL	*Business Workflow: Inbox Using POWL*
SAP_DAL_DEMO_ROLE_1	*SAP Desktop Application Launcher Demo Role #1*
SAP_DAL_DEMO_ROLE_2	*SAP Desktop Application Launcher Demo Role #2*
SAP_GRC_FN_ADISSUE_PROCESS	*Ad-hoc Issue Processer*
SAP_GRC_FN_ALL	*GRC - Power User*
SAP_GRC_FN_ALL	*GRC - Power User*
SAP_GRC_FN_BASE	*GRC - Base role to run GRC applications*
SAP_GRC_FN_BASE	*GRC - Base role to run GRC applications*
SAP_GRC_FN_BUSINESS_USER	*GRC - Business User*
SAP_GRC_FN_BUSINESS_USER	*GRC - Business User*
SAP_GRC_FN_DISPLAY	*GRC - Display*
SAP_GRC_FN_POST	*Role with Post Authority Only*

Step 2: In SAP NetWeaver Business Client, go to IAM Work Center.



Work Inbox

View all GRC workflow tasks assigned to you

Quick Links
Work Inbox

Application Help

Application Help for GRC Applications

Quick Links
Access Control

My Delegation

Delegate temporary approval of your workflow tasks to another person

Quick Links
Approver Delegation

My Profile

Create and track your access requests, view your access assignments, and manage your security settings

Quick Links
My Profile
Request Status
Reset Password
Name Change
Register Security Questions
Access Request

Step 3: Navigate to Internal Audit Management -> Audit Universe

Step 4: Click on **Create** button and go to **General** tab.

Step 5: Enter the following details for auditable entity:

- Name
- Description
- Type
- Status
- Notes to add any additional information

Step 6: Go to **Audit Plan** tab to view audit proposals and audit plan proposals with the transfer date.

Step 7: Select the **attachments and links** tab to add any type of files or links.

Step 8: When you enter the required details, you can select from the following options:

- Select **Save** to save the entity.
- Select **Close** to exit without saving.

SAP Process Control — Audit Risk Rating

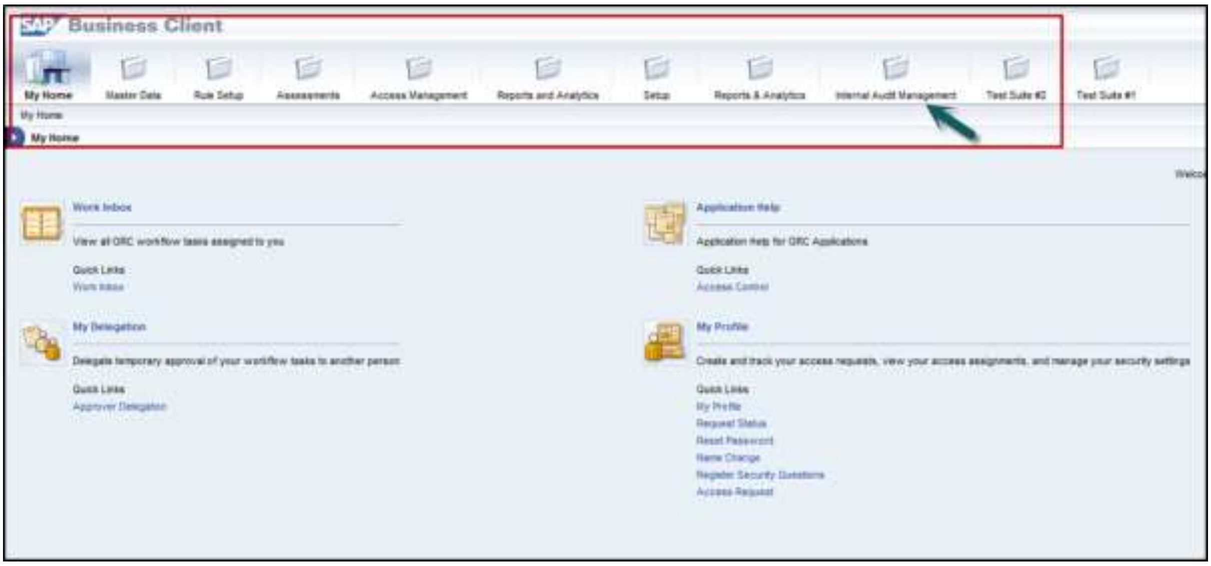
Audit Risk rating is used to define the criteria for an organization to find risk rating and establish ranking for risk rating. Each auditable entity is rated as per management feedback in ARR. You can use ARR to perform the following functions:

- You can find the set of auditable entities and risk factors.
- Define and evaluate risk scores for risk factor in each auditable entity.
- As per risk score, you can rate the auditable entity.
- You can also generate an audit plan from ARR by comparing risk scores for different auditable entities. In addition to this, you can select the high risk score auditable entities and generate audit proposal and audit plan proposal.

Create an Audit Risk Rating

Let us now understand the steps to create an Audit Risk Rating

Step 1: In SAP NetWeaver Business Client, go to IAM Work Center.



Work Inbox

View all GRC workflow tasks assigned to you

Quick Links
Work Inbox

My Delegation

Delegate temporary approval of your workflow tasks to another person

Quick Links
Approver Delegation

Application Help

Application Help for GRC Applications

Quick Links
Access Control

My Profile

Create and track your access requests, view your access assignments, and manage your security settings

Quick Links
My Profile
Request Status
Reset Password
Name Change
Register Security Questions
Access Request

Step 2: Navigate to Internal Audit Management -> Audit Risk Rating -> Create

Step 3: In General tab, enter the following details:

- Name
- Description
- Valid from
- Valid to
- Responsible person
- Status

Step 4: Go to Auditable Entities and click **Add** button to choose from auditable entities.

Step 5: Go to **Risk Factor** tab, and select **ARR** risk factor. Select **Add** to add a risk factor -> OK.

Step 6: Go to **Risk Scores** tab, select entity and input risk scores on risk factor table. Click **Calculate** button to view average score. Go to Risk level and risk priority column to enter the details.

Go to **Audit Plan Proposal** tab, to ensure that you are creating an audit plan proposal. Select export to create an excel spreadsheet to view information in table form for your ARR.

Select **Save** button to save audit risk rating for auditable entity.

11. SAP GRC — Process Control Work Centers

Work centers provide a central access point for the entire GRC functionality. They are organized to provide easy access to application activities, and contain menu groups and links to further activities.

The following work centers are shared by Access Control, Process Control and Risk Management:

- My Home
- Master Data
- Rule Setup
- Assessments
- Access Management
- Reports and Analytics

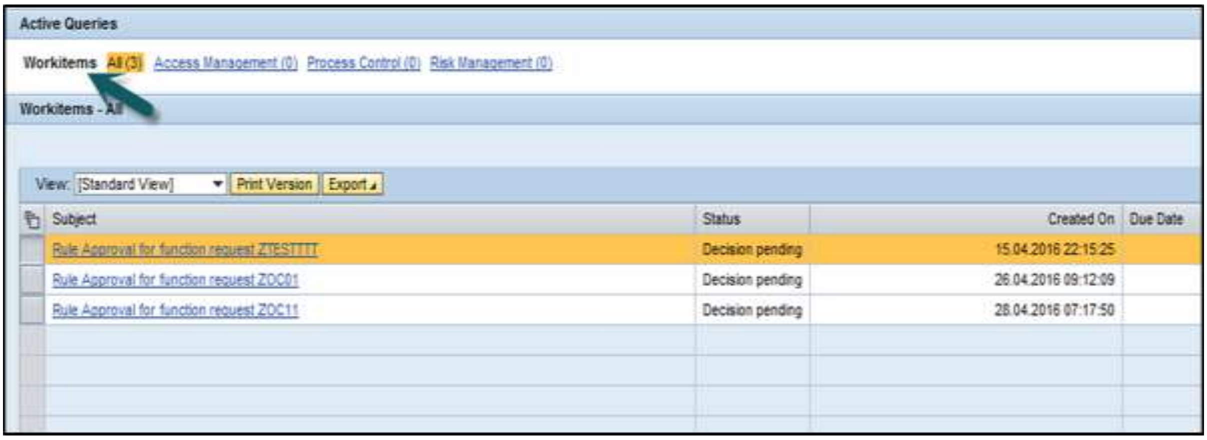
Let us discuss the major work centers.

My Home

My Home Work Center is shared by Process Control, Risk management and Access Control. This provides a centralized location where you can manage assigned tasks and accessible objects in GRC application. My Home comes with a number of sections. Let us now understand the Work Inbox section:

Work Inbox

Using Work Inbox, you can view the tasks that you have to process in GRC software.



Active Queries
Workitems All (3) Access Management (0) Process Control (0) Risk Management (0)
Workitems - All
View: [Standard View]
Print Version
Export

Subject	Status	Created On	Due Date
Rule Approval for function request ZTESTTTT	Decision pending	15.04.2016 22:15:25	
Rule Approval for function request ZOC01	Decision pending	26.04.2016 09:12:09	
Rule Approval for function request ZOC11	Decision pending	28.04.2016 07:17:50	

If you want to process a task, click on task in the table.

It will open the workflow window wherein, you can process the task.

Master Data

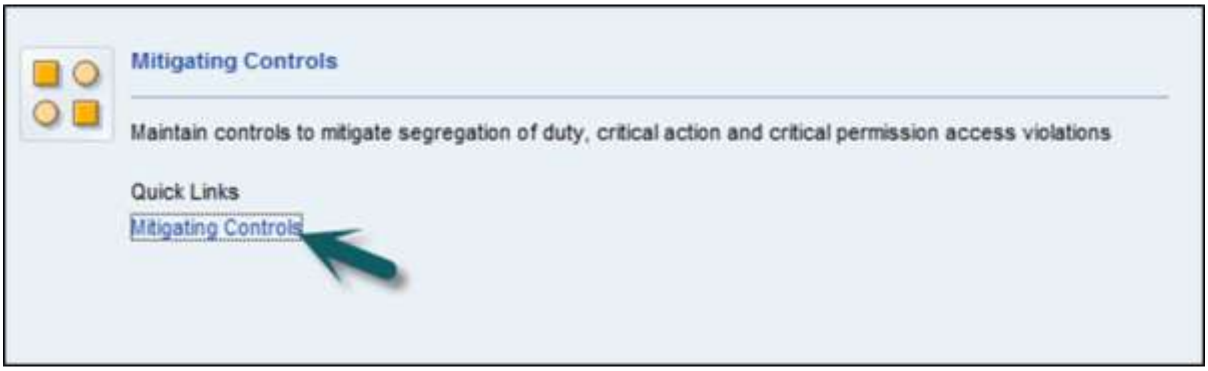
Master Data Work Center is shared by Process Control, Risk management and access control. The Process Control Master Data Work center contains the following sections:

- Organizations
- Regulations and Policies
- Objectives
- Activities and Processes
- Risks and Responses
- Accounts
- Reports

Let us now discuss the major work centers under Master Data Work Center:

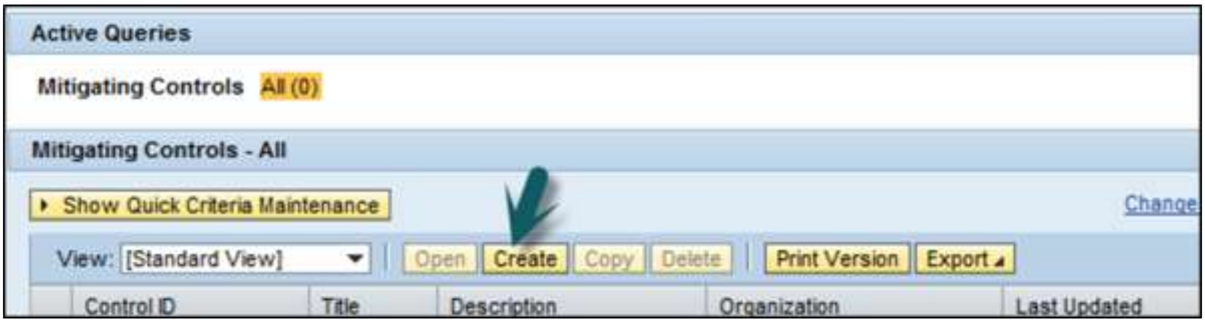
Organizations: Maintain the company's organization structure for compliance and risk management with related assignments

Mitigation Controls: Maintain controls to mitigate segregation of duty, critical action and critical permission access violations

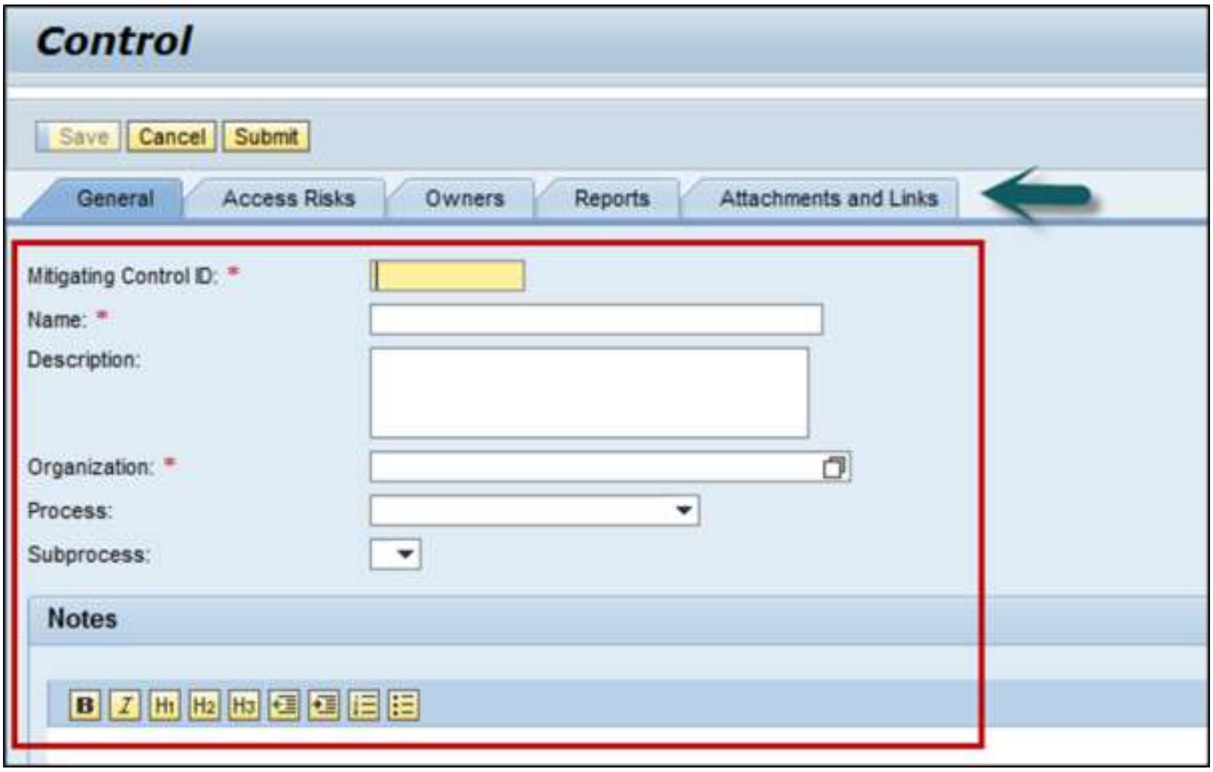

Mitigating Controls

Maintain controls to mitigate segregation of duty, critical action and critical permission access violations

To create mitigation control, click Create button.



You will be directed to a new window, enter the details for mitigation control and click Save button.



Reports and Analytics

Reports and Analytics Work Center is shared by Process Control, Risk management and Access Control. The Process Control Reports and Analytics Work Center consists of Compliance section in GRC application.

In compliance section, you can create the following reports under Process Control:

Evaluation Status Dashboard

Shows a high-level picture of the overall status of corporate compliance throughout different business entities and provides analytics and drilldown capabilities to view data on different levels and dimensions.

Survey Results

Displays the results of surveys.

Datasheet

Provides comprehensive information on master data, evaluation, and remediation activities for subprocesses and controls.

The following roles that use the datasheet functionality:

- **Internal Auditors:** They can use datasheets to get a picture of the controls and subprocesses in an organization under GRC.

- **Process Owners**: In GRC application, Process Owners and Control Owners can request datasheets to get an overview of their subprocesses. Datasheet information provides the definition of the subprocess, assessments completed on subprocess, controls encompassed by the subprocess, and the assessments and testing done on these controls.

- **Control Owners:** Control owners can use datasheets to check the design of their controls. Control owner can assess controls to check the controls and their effectiveness.

- **External Auditors:** Datasheets can be used by external auditors; this can be used to request the information to research controls or subprocesses.

Note: Other work centers like access management, assessments and rule set up are also share by process control, access control and risk management.

The Process Control Access Management Work Center has the GRC Role Assignments section.

12. SAP GRC — SoD Risk Management

In every business, it is required to perform Segregation of Duties (SoD) Risk Management — starting from risk recognition to rule building validation and various other risk management activities to follow continuous compliance.

As per different roles, there is a need to perform Segregation of Duties in GRC system. SAP GRC defines various roles and responsibilities under SoD Risk Management:

Business Process Owners

Business Process Owners perform the following tasks:

- Identify risks and approve risks for monitoring
- Approve remediation involving user access
- Design controls to mitigate conflicts
- Communicate access assignments or role changes
- Perform proactive continuous compliance

Senior Officers

Senior Officers perform the following tasks:

- Approve or reject risks between business areas
- Approve mitigation controls for selected risks

Security Administrators

Security Administrators perform the following tasks:

- Assume ownership of GRC tools and security process
- Design and maintain rules to identify risk conditions
- Customize GRC roles to enforce roles and responsibilities
- Analyze and remediate SoD conflicts at role level

Auditors

Auditors perform the following tasks:

- Risk assessment on a regular basis
- Provide specific requirements for audit purposes

- Periodic testing of rules and mitigation controls
- Act as liaison between external auditors

SoD Rule Keeper

SoD Rule Keeper performs the following tasks:

- GRC tool configuration and administration
- Maintains controls over rules to ensure integrity
- Acts as liaison bet ween basis and GRC support center

13. SAP GRC — Risk Management

SAP Risk Management in GRC is used to manage risk-adjusted management of enterprise performance that empowers an organization to optimize efficiency, increase effectiveness, and maximize visibility across risk initiatives.

The following are the **key functions** under Risk Management:

- Risk management emphasizes on organizational alignment towards top risks, associated thresholds, and risk mitigation.
- Risk analysis includes performing qualitative and quantitative analysis.
- Risk management involves Identification of key risks in an organization.
- Risk management also includes resolution/remediation strategies for risks.
- Risk management performs the alignment of key risk and performance indicators across all business functions permitting earlier risk identification and dynamic risk mitigation.

Risk management also involves proactive monitoring into existing business processes and strategies.

Phases in Risk Management

Let us now discuss the various phases in Risk Management. The following are the various phases in risk management:

- Risk Recognition
- Rule Building and Validation
- Analysis
- Remediation
- Mitigation
- Continuous Compliance

Risk Recognition

In a risk recognition process under risk management, the following steps can be performed:

- Identify authorization risks and approve exceptions

- Clarify and classify risk as high, medium or low
- Identify new risks and conditions for monitoring in the future

Rule Building and Validation

Perform the following tasks under Rule Building and Validation:

- Reference the best practices rules for environment
- Validate the rules
- Customize rules and test
- Verify against test user and role cases

Analysis

Perform the following tasks under Analysis:

- Run the analytical reports
- Estimate cleanup efforts
- Analyze roles and users
- Modify rules based on analysis
- Set alerts to distinguish executed risks

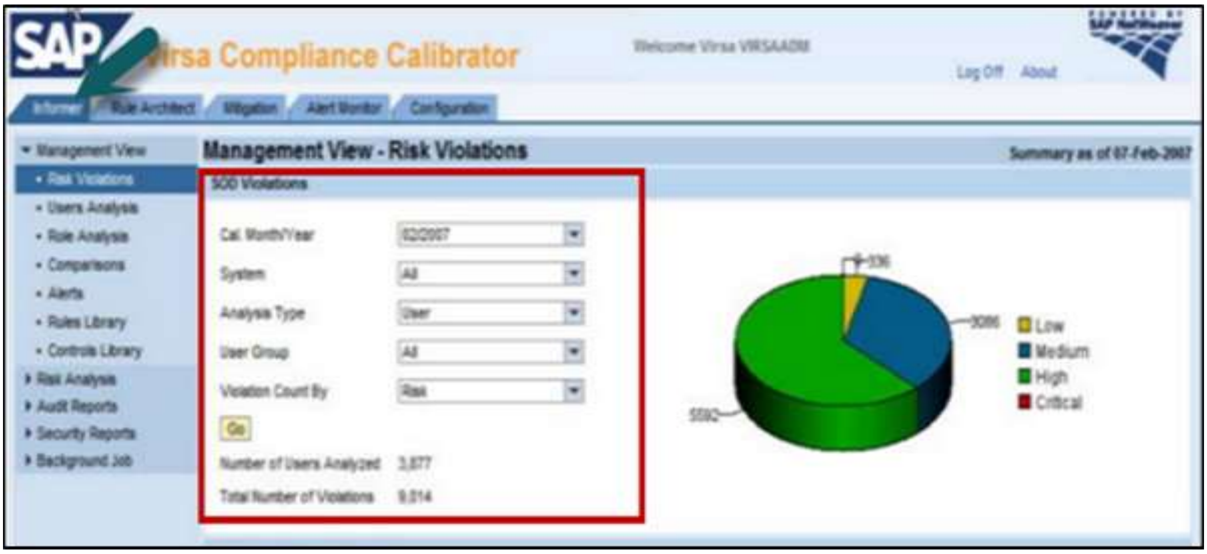
From the management aspect, you can see compact view of risk violations that are grouped by severity and time.

Step 1: Go to Virsa Compliance Calibrator -> Informer tab

Step 2: For SoD violations, you can display a pie chart and a bar chart to represent current and past violations in the system landscape.

The following are the two different views to these violations:

- Violations by risk level
- Violations by process



Management View - Risk Violations

Summary as of 07-Feb-2007

SOD Violations

Cal. Month/Year: 02/2007

System: All

Analysis Type: User

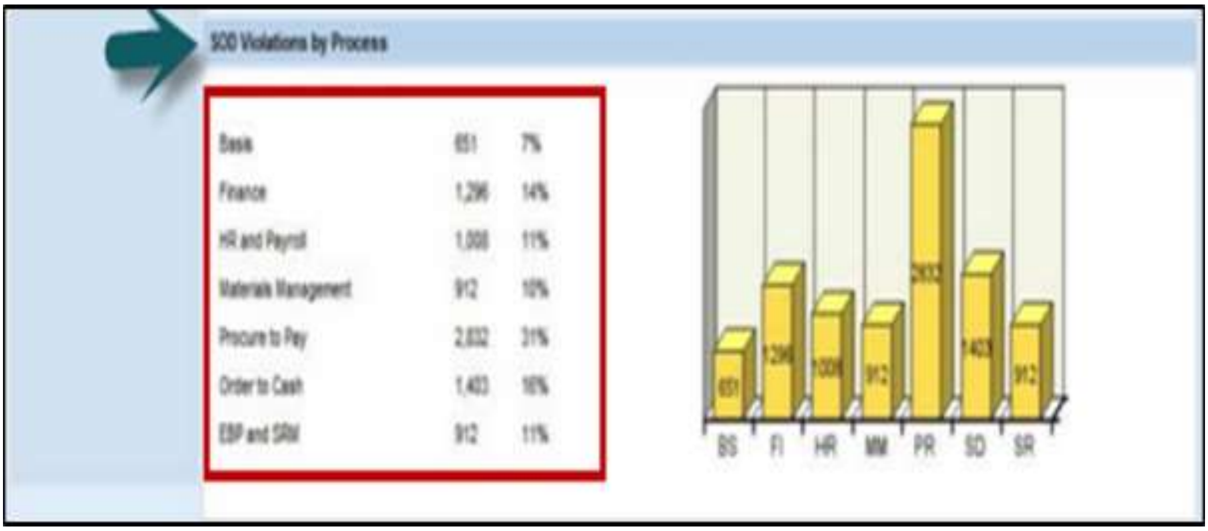
User Group: All

Violation Count By: Risk

Go

Number of Users Analyzed 3,877

Total Number of Violations 9,014



SOD Violations by Process

Basis	651	7%
Finance	1,296	14%
HR and Payroll	1,008	11%
Materials Management	912	10%
Procure to Pay	2,832	31%
Order to Cash	1,403	16%
ESP and SRM	912	11%

Remediation

Perform the following tasks under remediation:

- Determine alternatives for eliminating risks
- Present analysis and select corrective actions
- Document approval of corrective actions
- Modify or create roles or user assignments

Mitigation

Perform the following tasks under mitigation:

- Determine alternative controls to mitigate risk

- Educate management about conflict approval and monitoring
- Document a process to monitor mitigation controls
- Implement controls

Continuous Compliance

Perform the following tasks under Continuous Compliance:

- Communicate changes in roles and user assignments
- Simulate changes to roles and users
- Implement alerts to monitor for selected risks and mitigate control testing

Risk Classification

Risks should be classified as per the company policy. The following are the various risk classifications that you can define as per risk priority and company policy:

Critical

Critical classification is done for risks that contain company’s critical assets that are very likely to be compromised by fraud or system disruptions.

High

This includes physical or monetary loss or system-wide disruption that includes fraud, loss of any asset or failure of a system.

Medium

This includes multiple system disruption like overwriting master data in the system.

Low

This includes risk where the productivity losses or system failures compromised by fraud or system disruptions and loss is minimum.

14. SAP GRC — Risk Remediation

In SAP GRC 10.0 Risk Management, risk remediation phase determines the method to eliminate risks in roles. The purpose of the remediation phase is to determine alternatives for eliminating issues under risk management.

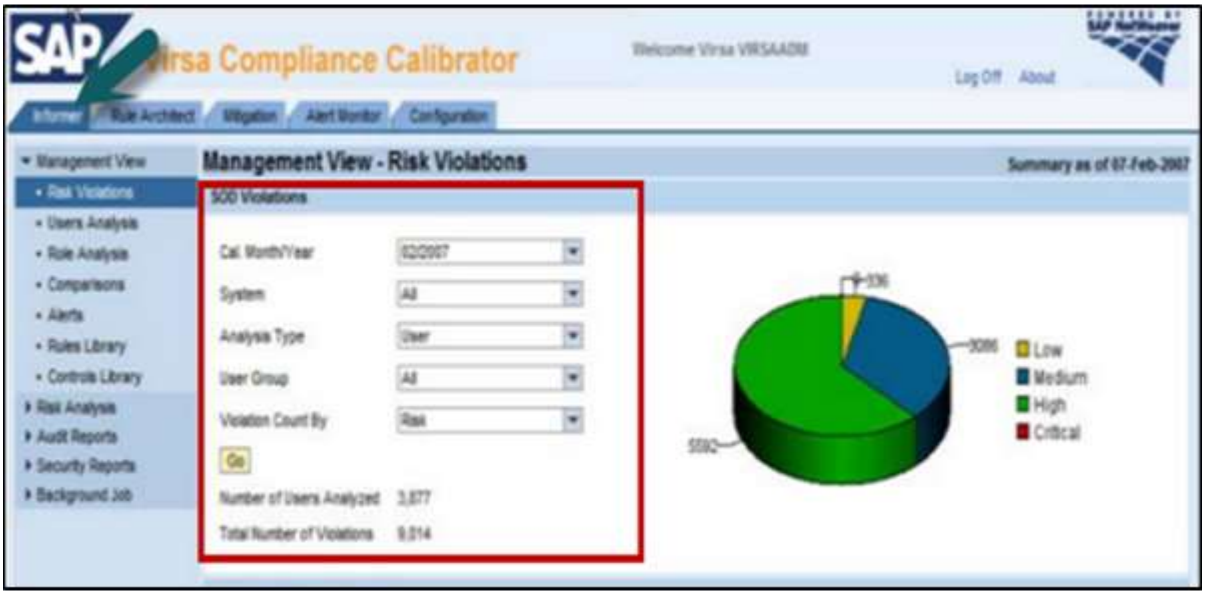
The following approaches are recommended to resolve issues in roles:

Single Roles

- You can start with single roles as it is easy and simplest way to start.
- You can check for any Segregation of Duties SoD violations from being reintroduced.

Composite roles

- You can perform various analysis to check the user assignment on the assignment or removal of user actions.
- You can use Management view or Risk Analysis reports for analysis as mentioned in previous topic.



Management View - Risk Violations

Summary as of 07-Feb-2007

SOD Violations

Cal. Month/Year: 02/2007

System: All

Analysis Type: User

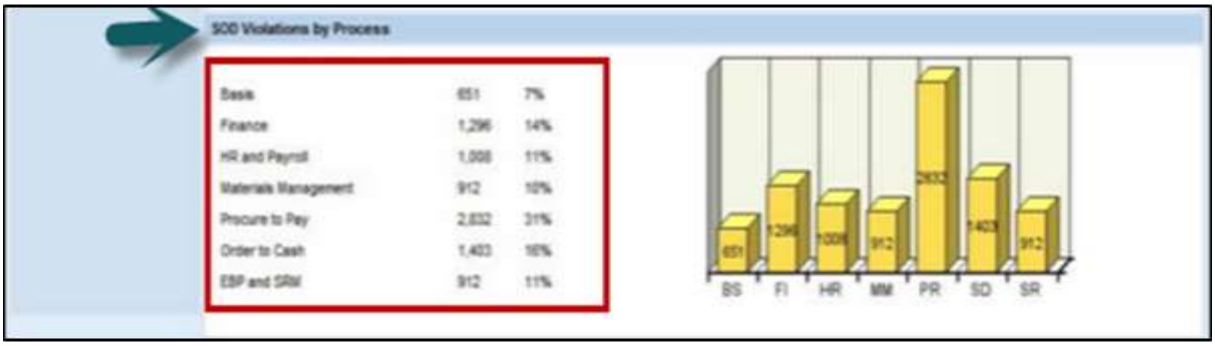
User Group: All

Violation Count By: Risk

Go

Number of Users Analyzed 3,877

Total Number of Violations 9,014


SOD Violations by Process

Basis	651	7%
Finance	1,296	14%
HR and Payroll	1,008	11%
Materials Management	912	10%
Procure to Pay	2,832	31%
Order to Cash	1,403	16%
EBP and SRM	912	11%

In Risk Remediation, Security Administrators should document the plan and Business Process Owners should be involved and approve the plan.

SAP GRC — Report Type

You can generate different Risk Analysis reports as per the required analysis:

- **Action Level** – You can use it to perform SoD analysis at action level.

- **Permission Level** – This can be used to perform SoD analysis at action and permission levels.

- **Critical Actions** – This can be used to analyze the users who have access to one of the critical functions.

- **Critical Permissions** – This can be used to analyze users having access to one critical function.

- **Critical Roles/Profiles** – This can be used to analyze the users who has access to critical roles or profiles.

15. SAP GRC — Mitigation Controls

In SAP GRC 10.0, you can use mitigation controls when it is not possible to separate Segregation of duties SoD from the business process.

Example

In an organization, consider a scenario where a person takes care of roles within business processes that cause a missing SoD conflict.

There are different examples that are possible for mitigation controls:

- Release strategies and authorization limits
- Review of user logs
- Review of exception reports
- Detailed variance analysis
- Establish insurance to cover impact of a security incident

Mitigation Control Types

There are two types of mitigation control under SAP GRC Risk management:

- Preventive
- Detective

Preventive Mitigation Controls

Preventive mitigation control is used to reduce the impact of risk before it actually occurs. There are various activities that you can perform under preventive mitigation control:

- Configuration
- User Exits
- Security
- Defining workflow
- Custom Objects

Detective Mitigation Controls

Detective mitigation control is used when an alert is received and a risk occurs. In this case, the person who is responsible to initiate corrective measure mitigates the risk.

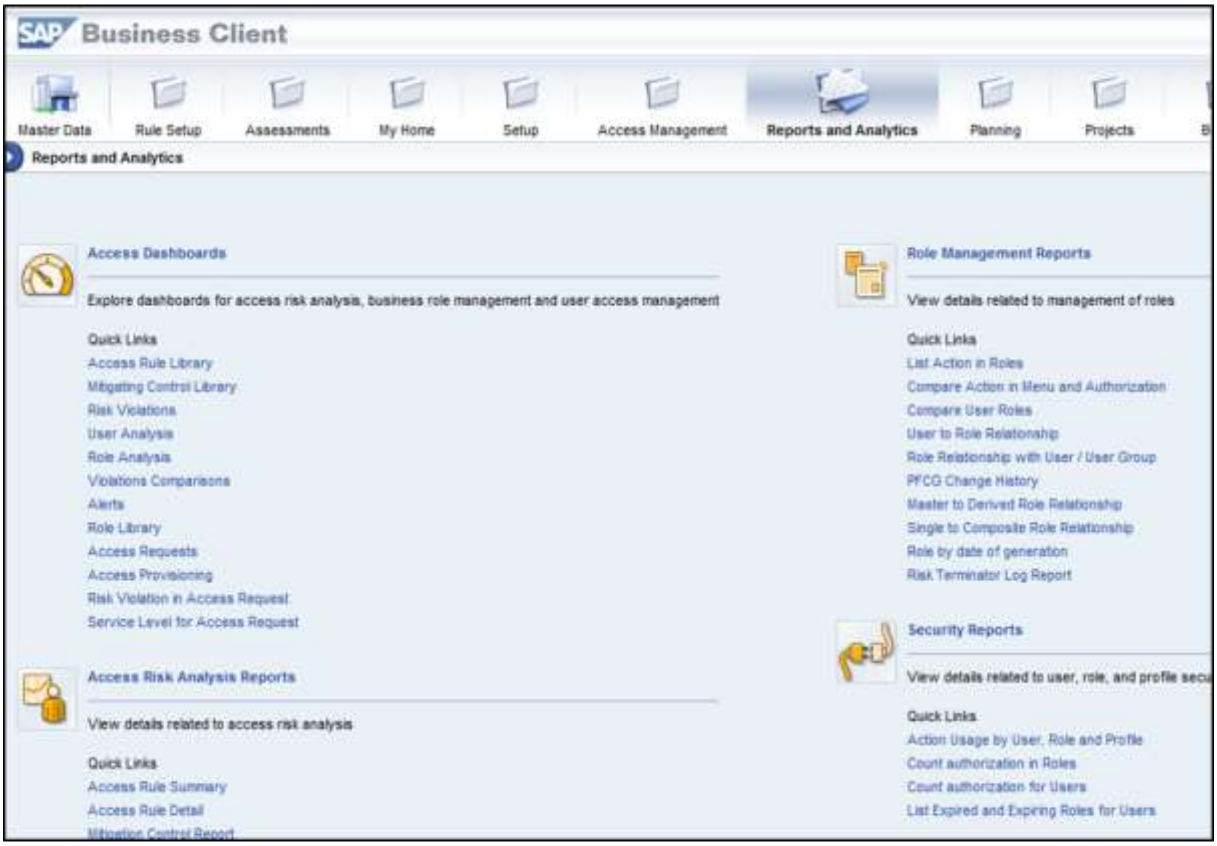
There are various activities that you can perform under detective mitigation control:

- Activity Reports
- Comparison of plan vs actual review
- Budget review
- Alerts

Setting up Migration Controls

Follow these steps to set up migration controls:

Step 1: Login to SAP GRC Access control.



Access Dashboards

Explore dashboards for access risk analysis, business role management and user access management

Quick Links
Access Rule Library
Mitigating Control Library
Risk Violations
User Analysis
Role Analysis
Violations Comparisons
Alerts
Role Library
Access Requests
Access Provisioning
Risk Violation in Access Request
Service Level for Access Request

Access Risk Analysis Reports

View details related to access risk analysis

Quick Links
Access Rule Summary
Access Rule Detail
Mitigation Control Report

Role Management Reports

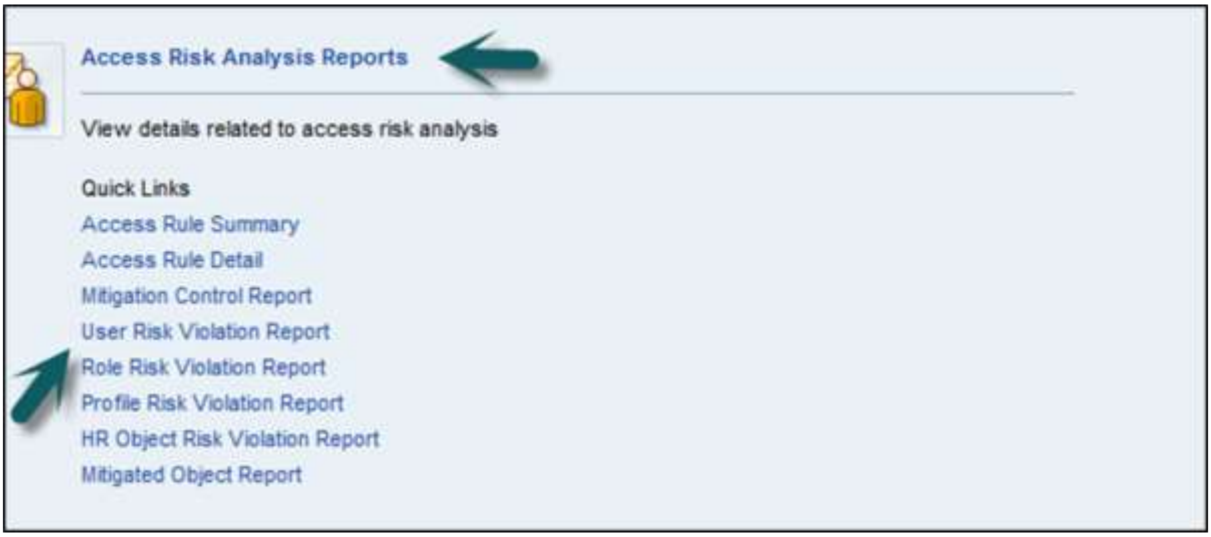
View details related to management of roles

Quick Links
List Action in Roles
Compare Action in Menu and Authorization
Compare User Roles
User to Role Relationship
Role Relationship with User / User Group
PFCG Change History
Master to Derived Role Relationship
Single to Composite Role Relationship
Role by date of generation
Risk Terminator Log Report

Security Reports

View details related to user, role, and profile secu

Quick Links
Action Usage by User, Role and Profile
Count authorization in Roles
Count authorization for Users
List Expired and Expiring Roles for Users



Access Risk Analysis Reports

View details related to access risk analysis

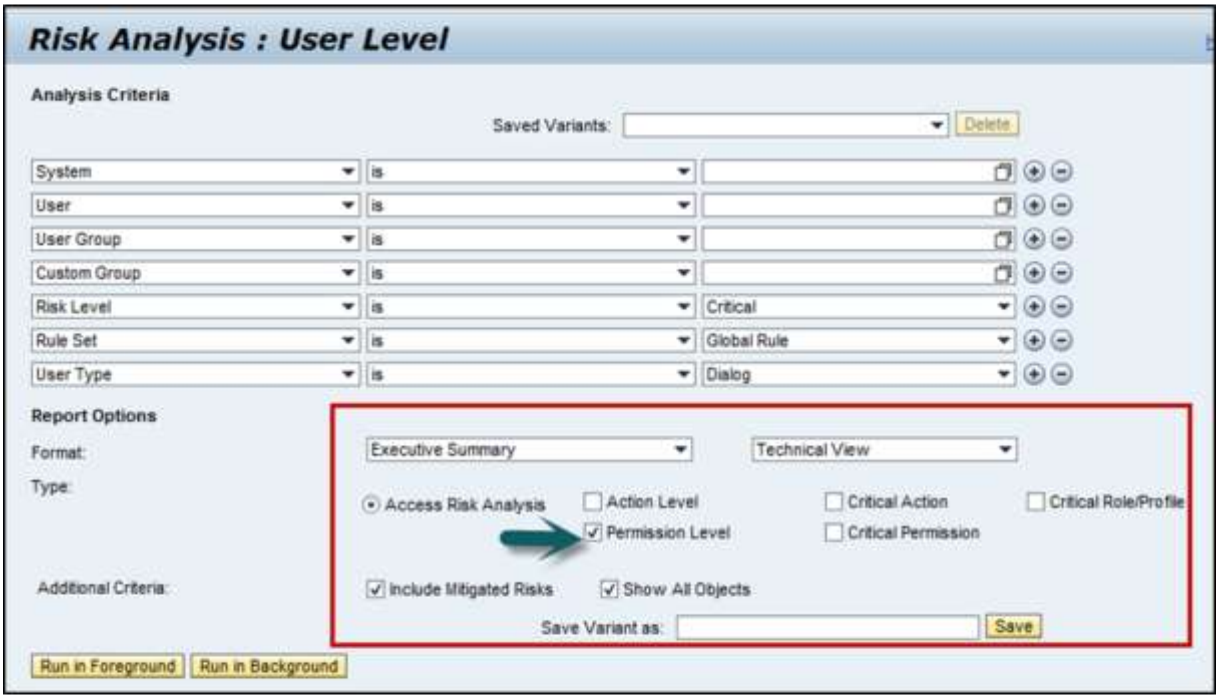
Quick Links

- Access Rule Summary
- Access Rule Detail
- Mitigation Control Report
- User Risk Violation Report
- Role Risk Violation Report
- Profile Risk Violation Report
- HR Object Risk Violation Report
- Mitigated Object Report

Step 2: Perform a risk analysis on user level. Enter the below details:

- Report Type
- Report Format

Step 3: Click Execute.



Risk Analysis : User Level

Analysis Criteria

Saved Variants: Delete

System	is	
User	is	
User Group	is	
Custom Group	is	
Risk Level	is	Critical
Rule Set	is	Global Rule
User Type	is	Dialog

Report Options

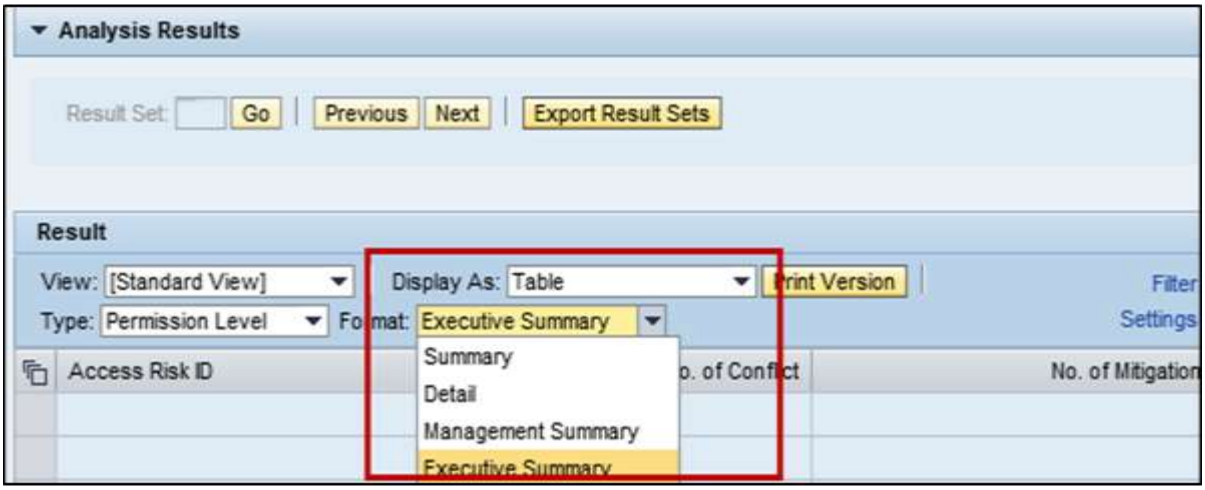
Format: Executive Summary Technical View

Type: ● Access Risk Analysis □ Action Level ☑ Permission Level □ Critical Action □ Critical Permission □ Critical Role/Profile

Additional Criteria: ☑ Include Mitigated Risks ☑ Show All Objects

Save Variant as: Save

Step 4: You can toggle between different report types as in the following screenshot:

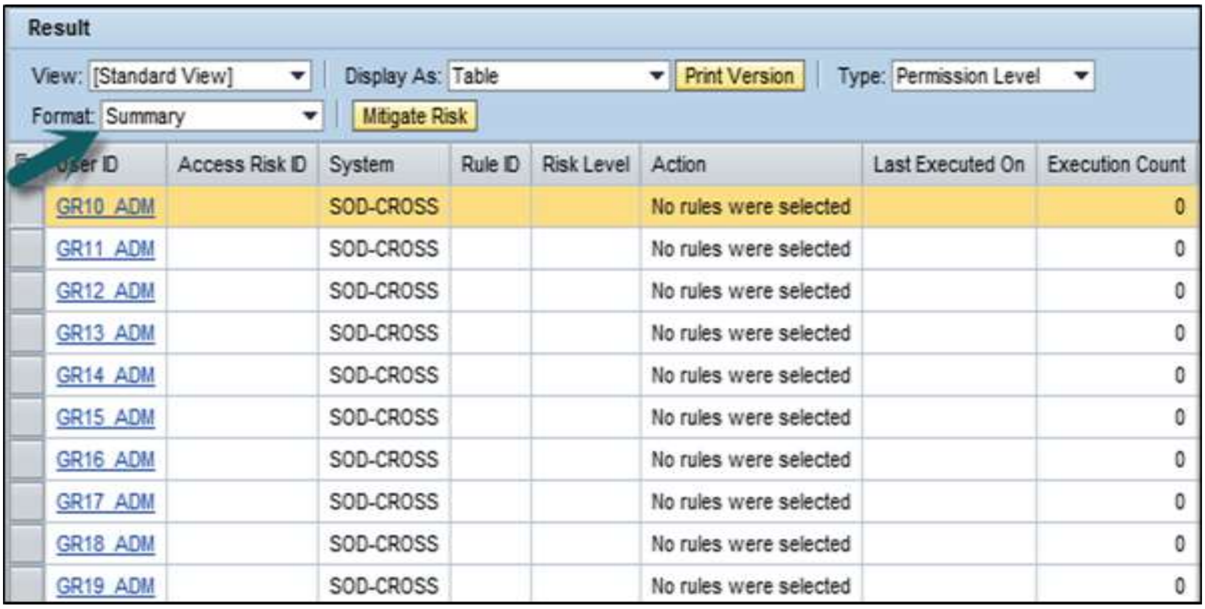


View: [Standard View]

Display As: Table

Type: Permission Level

Format: Executive Summary



View: [Standard View]

Display As: Table

Type: Permission Level

Format: Summary

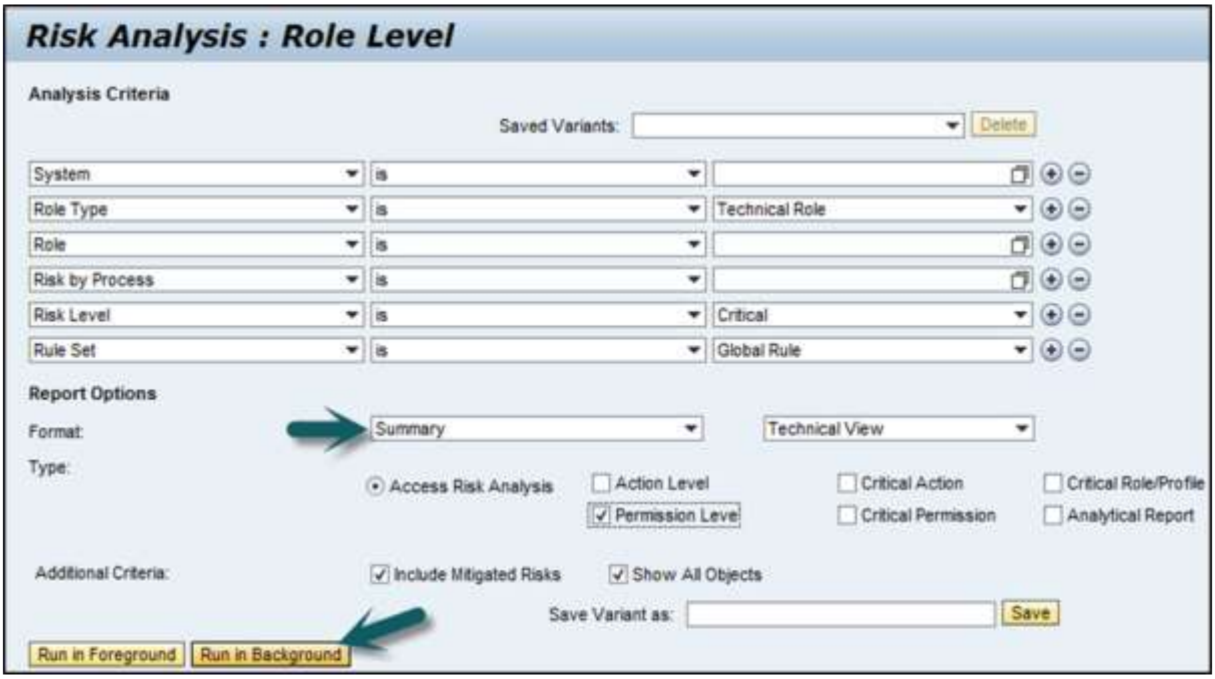
User ID	Access Risk ID	System	Rule ID	Risk Level	Action	Last Executed On	Execution Count
GR10_ADM		SOD-CROSS			No rules were selected		0
GR11_ADM		SOD-CROSS			No rules were selected		0
GR12_ADM		SOD-CROSS			No rules were selected		0
GR13_ADM		SOD-CROSS			No rules were selected		0
GR14_ADM		SOD-CROSS			No rules were selected		0
GR15_ADM		SOD-CROSS			No rules were selected		0
GR16_ADM		SOD-CROSS			No rules were selected		0
GR17_ADM		SOD-CROSS			No rules were selected		0
GR18_ADM		SOD-CROSS			No rules were selected		0
GR19_ADM		SOD-CROSS			No rules were selected		0

Step 5: Logon to SAP GRC Access Control and schedule a risk analysis background job on role level.

Enter the following details:

- Report Type: Permission Level
- Report Format: Summary

Step 6: Click **Run in Background** as shown in the following screenshot:



Risk Analysis : Role Level

Analysis Criteria

Saved Variants:

System	is	
Role Type	is	Technical Role
Role	is	
Risk by Process	is	
Risk Level	is	Critical
Rule Set	is	Global Rule

Report Options

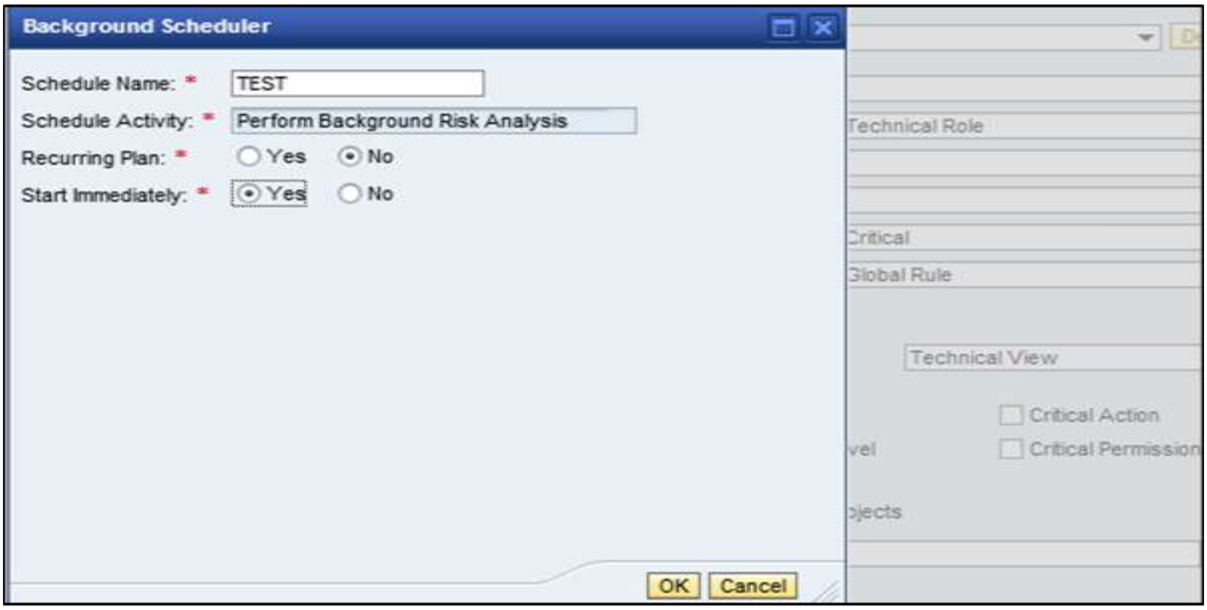
Format: Summary | Technical View

Type: ● Access Risk Analysis □ Action Level ☑ Permission Leve □ Critical Action □ Critical Permission □ Critical Role/Profile □ Analytical Report

Additional Criteria: ☑ Include Mitigated Risks ☑ Show All Objects

Save Variant as:

Step 7: In the next window, you can select **Start Immediately**. Then, click **OK**.



Background Scheduler

Schedule Name: * TEST

Schedule Activity: * Perform Background Risk Analysis

Recurring Plan: * ○ Yes ● No

Start Immediately: * ● Yes ○ No

16. SAP GRC — Superuser Privilege

In SAP GRC 10.0, Superuser Privilege Management needs to be implemented in your organization to eliminate the excessive authorizations and risks that your company experiences with the current emergency user approach.

The following are the key features in Superuser Privilege:

- You can allow Superuser to perform emergency activities within a controlled and auditable environment
- Using Superuser, you can report all the user activities accessing higher authorization privileges.
- You can generate an audit trail, which can be used to document reasons for using higher access privileges.
- This audit trail can be used for SOX compliance.
- Superuser can act as firefighter and have the following additional capabilities:
  - It can be used to perform tasks outside of their normal role or profile in an emergency situation.
  - Only certain individuals (owners) can assign Firefighter IDs.
  - It provides an extended capability to users while creating an auditing layer to monitor and record usage.

Standard Roles under Superuser Privilege Management

You can use the following standard roles for Superuser Privilege Management:

/VIRSA/Z_VFAT_ADMINISTRATOR

- This has the Ability to configure Firefighter
- Assign Firefighter role owners and controllers to Firefighter IDs
- Run Reports

/VIRSA/Z_VFAT_ID_OWNER

- Assign Firefighter IDs to Firefighter users
- Upload, download, and view Firefighter history log

VIRSA/Z_VFAT_FIREFIGHTER

- Access the firefighter program

17. SAP GRC — Implementing Superuser

Let us now understand how to implement Superuser.

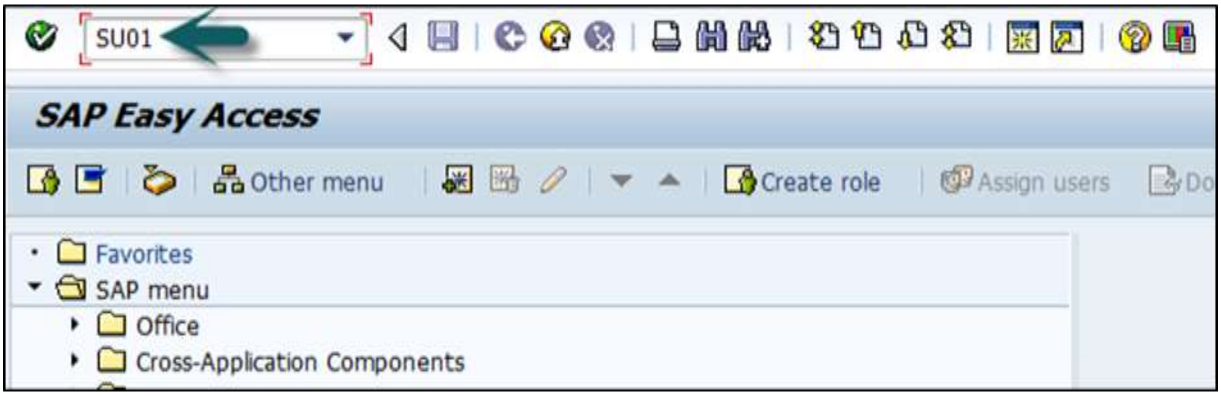
You can implement firefighter IDs by working on the following steps:

Step 1: Create Firefighter IDs for each business process area

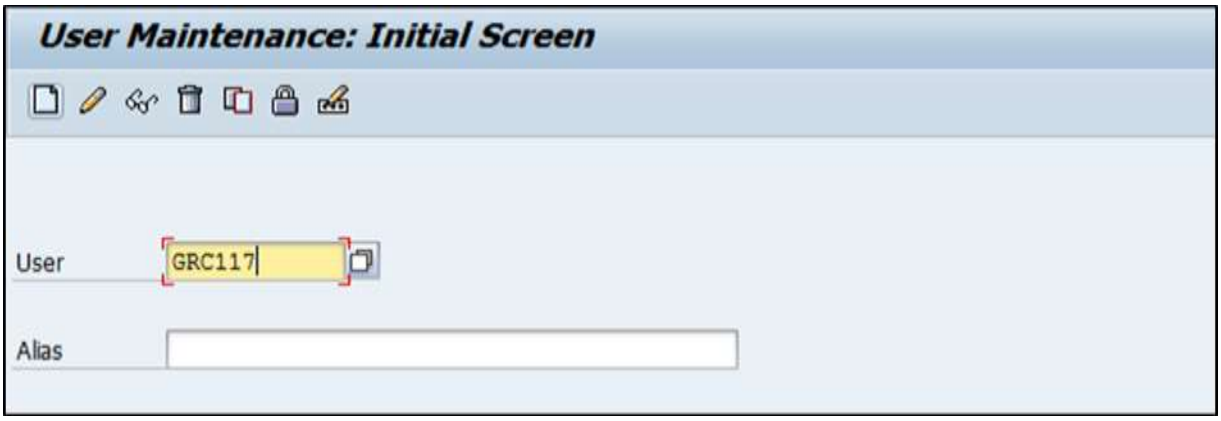
Step 2: Assign necessary roles and profiles to carry firefighting tasks.

You shouldn't assign profile SAP_ALL

Step 3: Use T-Code – SU01



Step 4: Click **Create** button to create a new user.


User Maintenance: Initial Screen

User GRC117

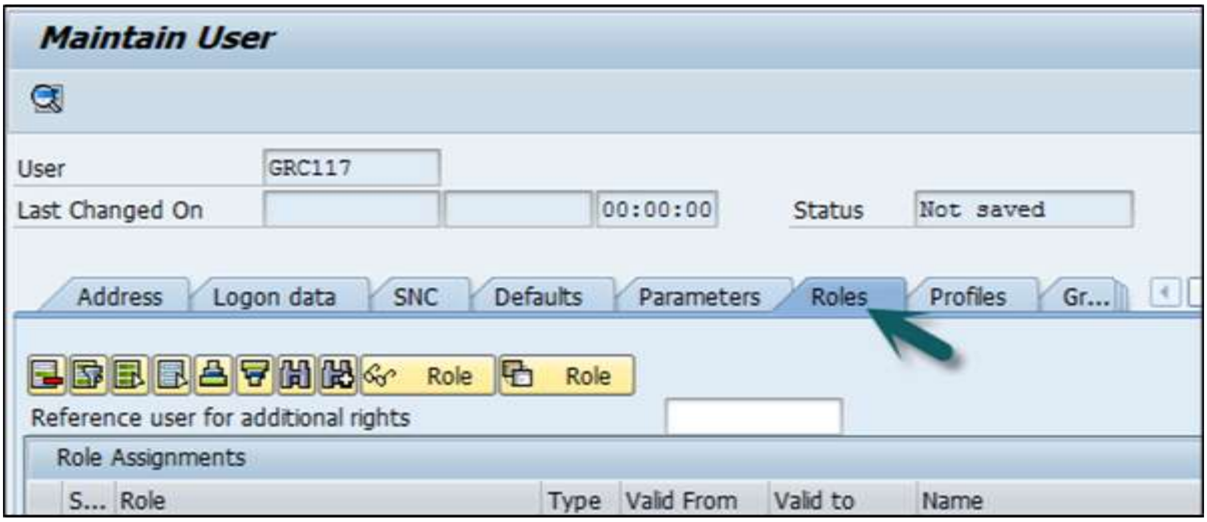
Alias

Step 5: Assign Firefighter roles as mentioned above to user id:

- Assign Firefighter roles to applicable user IDs.
- Assign administrator role /VIRSA/Z_VFAT_ADMINISTRATOR to superuser privilege management administrator:
- Administrator user should not be assigned any firefighting

- Assign the standard role /VIRSA/ Z_VFAT_FIREFIGHTER to:
  - ○ **Firefighter ID:** Service user used for logon
  - ○ **Firefighter user:** Standard user acting as a Firefighter in case
- Assign the ID owner role /VIRSA/Z_VFAT_ID_OWNER to:
  - ○ Owner: Responsible for determining who will be assigned to
  - ○ Controller: Receives notification when the Firefighter ID is responsibilities of emergency Firefighter IDs for his or her business area used.

Step 6: Go to **Roles** tab and select the mentioned roles as per the requirement.



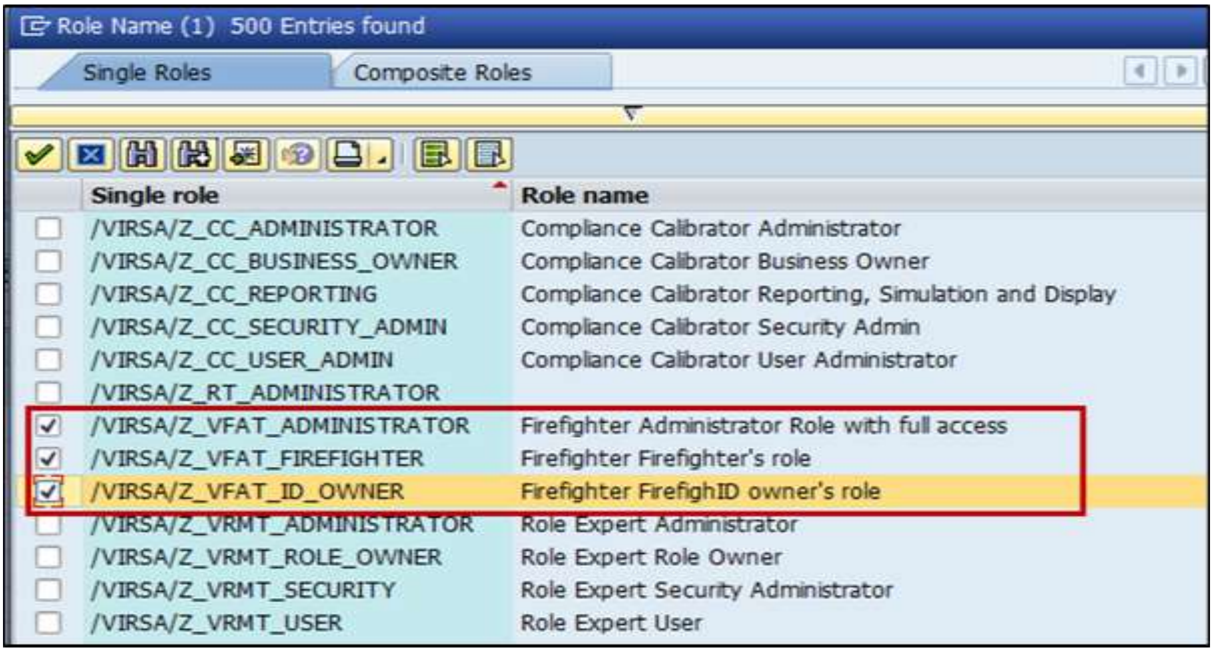
Maintain User

User	GRC117		
Last Changed On	00:00:00	Status	Not saved

Reference user for additional rights

Role Assignments

S...	Role	Type	Valid From	Valid to	Name



Role Name (1) 500 Entries found

	Single role	Role name
□	/VIRSA/Z_CC_ADMINISTRATOR	Compliance Calibrator Administrator
□	/VIRSA/Z_CC_BUSINESS_OWNER	Compliance Calibrator Business Owner
□	/VIRSA/Z_CC_REPORTING	Compliance Calibrator Reporting, Simulation and Display
□	/VIRSA/Z_CC_SECURITY_ADMIN	Compliance Calibrator Security Admin
□	/VIRSA/Z_CC_USER_ADMIN	Compliance Calibrator User Administrator
□	/VIRSA/Z_RT_ADMINISTRATOR	
☑	/VIRSA/Z_VFAT_ADMINISTRATOR	Firefighter Administrator Role with full access
☑	/VIRSA/Z_VFAT_FIREFIGHTER	Firefighter Firefighter's role
☑	/VIRSA/Z_VFAT_ID_OWNER	Firefighter FirefighID owner's role
□	/VIRSA/Z_VRMT_ADMINISTRATOR	Role Expert Administrator
□	/VIRSA/Z_VRMT_ROLE_OWNER	Role Expert Role Owner
□	/VIRSA/Z_VRMT_SECURITY	Role Expert Security Administrator
□	/VIRSA/Z_VRMT_USER	Role Expert User

Step 7: Create RFC destination for internal switch to Firefighter ID:

- Name: Enter RFC connection name

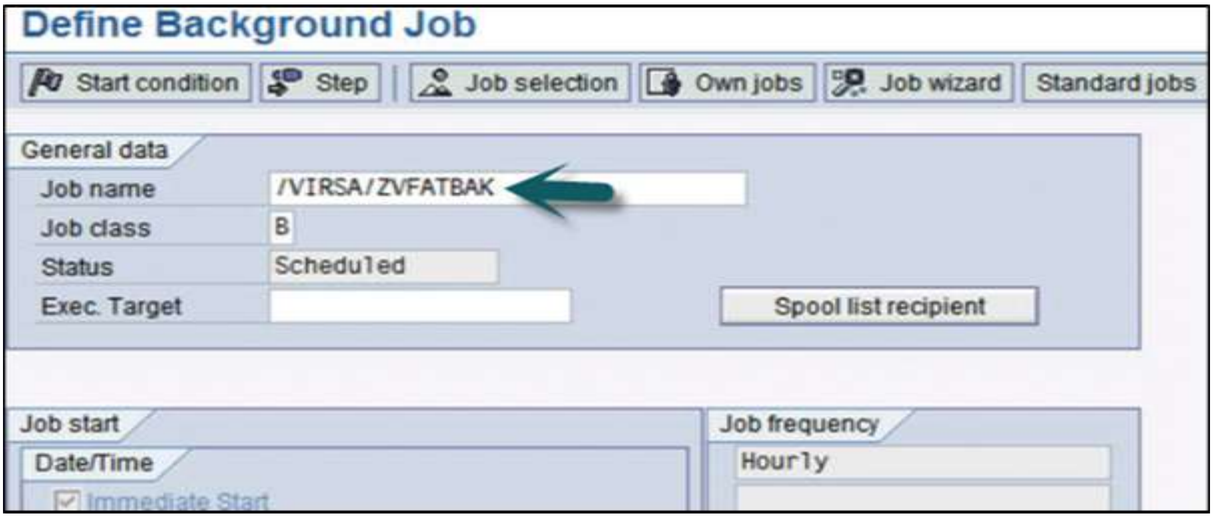
- Connection Type: 3

- Enter a Description
  (No username, passwords, or other logon data are required)

- Enter passwords for each Firefighter ID in the Security table: Passwords are stored as hash values and are unreadable after the administrator saves the value.

Step 8: To create firefighter log, you can schedule a background job.

Name the job **/VIRSA/ZVFATBAK** as in the following screenshot:



Define Background Job

General data

Job name: /VIRSA/ZVFATBAK

Job class: B

Status: Scheduled

Exec. Target:

Job start

Date/Time

☑ Immediate Start

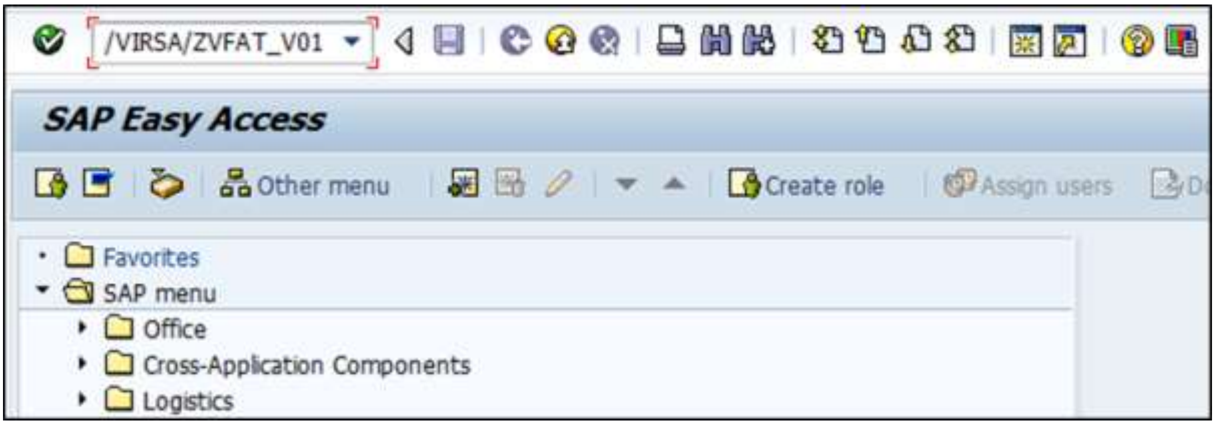
Job frequency

Hourly

Superuser Log

Let us understand these steps for Superuser Log.

Step 1: Use T-Code: Transaction: /n/VIRSA/ZVFAT_V01

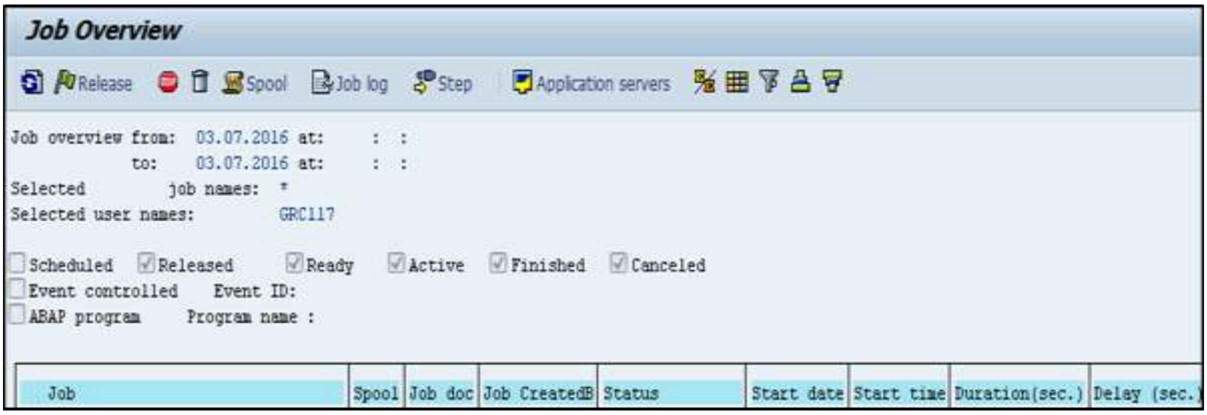


/VIRSA/ZVFAT_V01

SAP Easy Access

Step 2: You can now find the logs in the toolbox area. .

Step 3: You can use **transaction code — SM37** to review the logs for individual user.



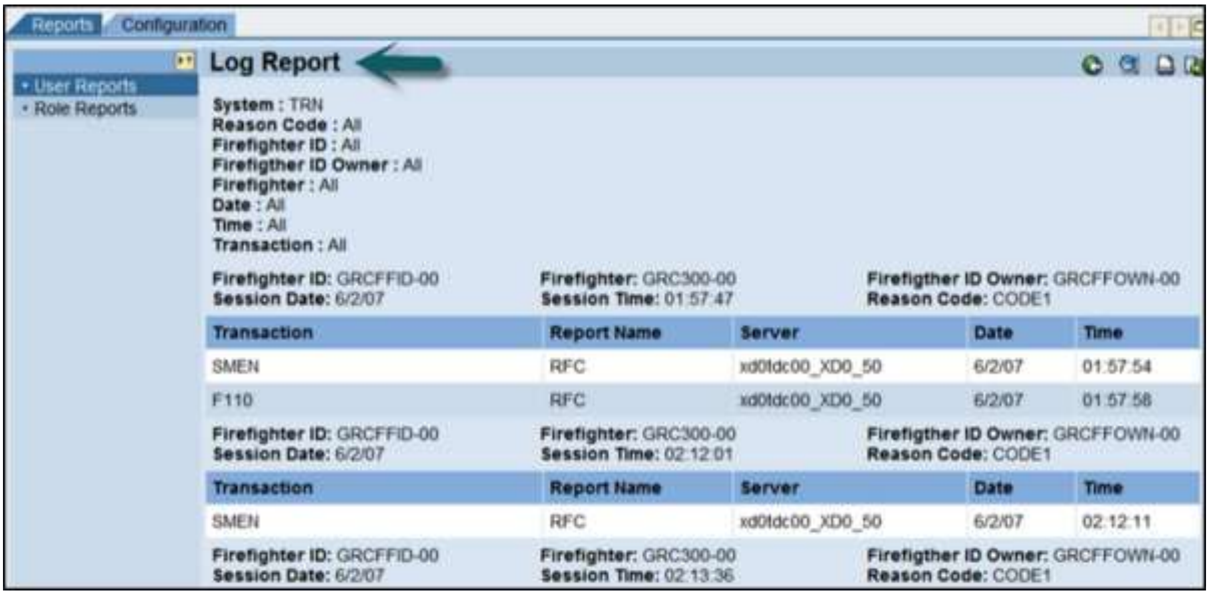
Job overview from: 03.07.2016 at: : :
to: 03.07.2016 at: : :
Selected job names: *
Selected user names: GRC117

☐ Scheduled ☑ Released ☑ Ready ☑ Active ☑ Finished ☑ Canceled
☐ Event controlled Event ID:
☐ ABAP program Program name :

Job	Spool	Job doc	Job CreatedB	Status	Start date	Start time	Duration(sec.)	Delay (sec.)

You can also use the web GUI to access all Firefighter information. Go to SAP GRC Access control -> Superuser privilege management.

So it is possible to access the data of different Firefighter installations on different SAP backend systems. And **it is not necessary to log on to each system anymore**.



Log Report

System : TRN
Reason Code : All
Firefighter ID : All
Firefigther ID Owner : All
Firefighter : All
Date : All
Time : All
Transaction : All

Firefighter ID: GRCFFID-00 **Firefighter:** GRC300-00 **Firefigther ID Owner:** GRCFFOWN-00
Session Date: 6/2/07 **Session Time:** 01:57:47 **Reason Code:** CODE1

Transaction	Report Name	Server	Date	Time
SMEN	RFC	xd0tdc00_XD0_50	6/2/07	01:57:54
F110	RFC	xd0tdc00_XD0_50	6/2/07	01:57:58

Firefighter ID: GRCFFID-00 **Firefighter:** GRC300-00 **Firefigther ID Owner:** GRCFFOWN-00
Session Date: 6/2/07 **Session Time:** 02:12:01 **Reason Code:** CODE1

Transaction	Report Name	Server	Date	Time
SMEN	RFC	xd0tdc00_XD0_50	6/2/07	02:12:11

Firefighter ID: GRCFFID-00 **Firefighter:** GRC300-00 **Firefigther ID Owner:** GRCFFOWN-00
Session Date: 6/2/07 **Session Time:** 02:13:36 **Reason Code:** CODE1

18. SAP GRC — Enhanced Risk Analysis

You can implement enhanced risk analysis using organization rules. In shared service business units, you can use organization rules to achieve procedures for risk analysis and management of user groups.

Consider a case where a user has created a fictitious vendor and invoices have been generated to gain financial benefit.

You can create an organization rule with company code enabled to eliminate this scenario.

Following steps should be performed to prevent this situation:

- Enable organization level fields in functions
- Create org rules
- Update org user mapping table
- Configure risk analysis web service

Enable organization level fields in functions

Follow these steps to enable organization level fields in functions:

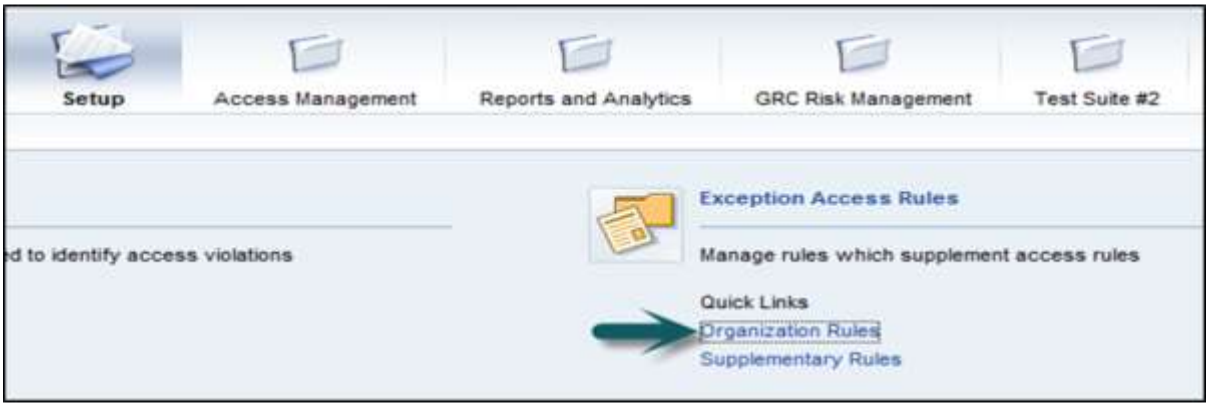
- Find out functions to be segregated by organization level in shared service environment.
- Maintain permissions for affected transactions.

Create organization rules

Follow these steps to create organization rules:

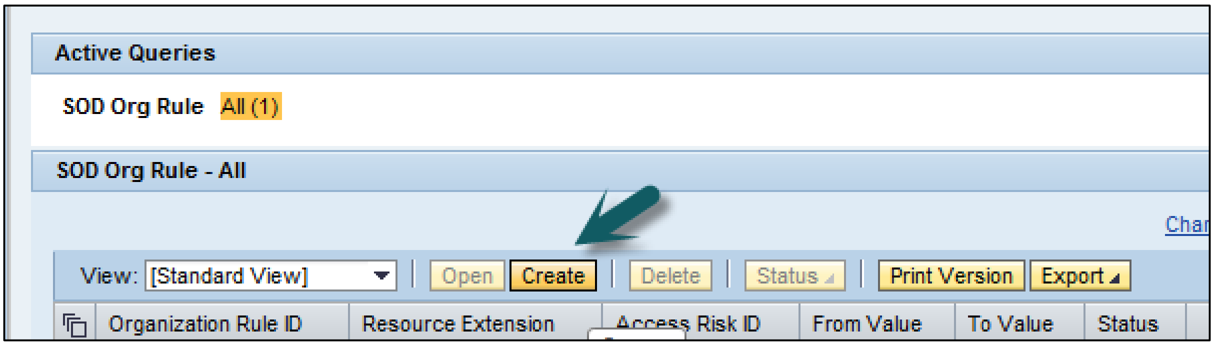
Step 1: Create organization rules for every possible value of organization field.

Step 2: Go to rule architect -> Organization level -> Create

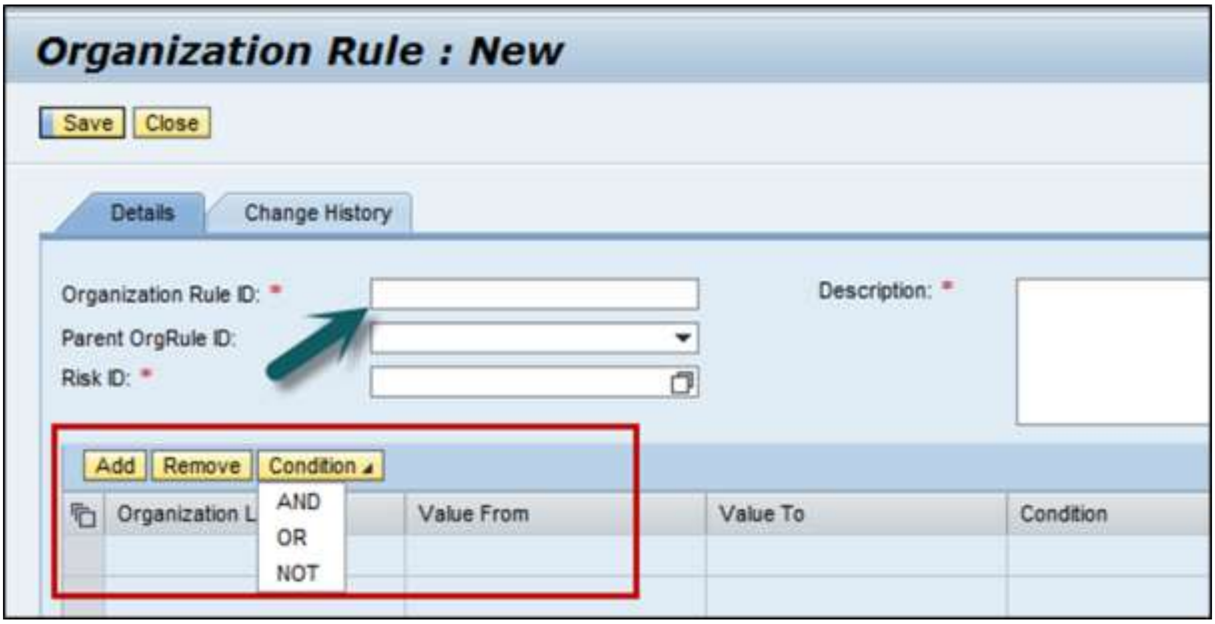


d to identify access violations

Manage rules which supplement access rules



Step 3: Enter the organization rule ID field.



Step 4: Enter the related task.

Step 5: Define organization level field and combine them with Boolean operators.

Step 6: Click **Save** button to save the Organization rule.

Benefits of Using Organization Rules

Let us now understand th benefits of using organization rules.

You can use organizational rules for companies to implement following features:

- You can use organization rules to implement shared services. They segregate duties with the help of organizational restrictions.

- Go to Risk Analysis -> Org Level

- Perform a risk analysis of analysis type Org Rule against a user

- You will receive the following output:
  - The risk analysis will only show a risk if the user has access to the same specific company code in each of the conflicting functions.

19. SAP GRC — Assigning Mitigation Controls

In an organization, you have control owners at different organization hierarchy levels. Risk should be managed and mitigated as per level of access.

The following are the control owners in an organization:

- One control owner for global level
- Different control owners for regional levels
- Multiple control owners for local level

You have to assign mitigation controls to different levels of responsibility. Now if there is a risk violation at region and local level, you should perform risk mitigation at highest level.

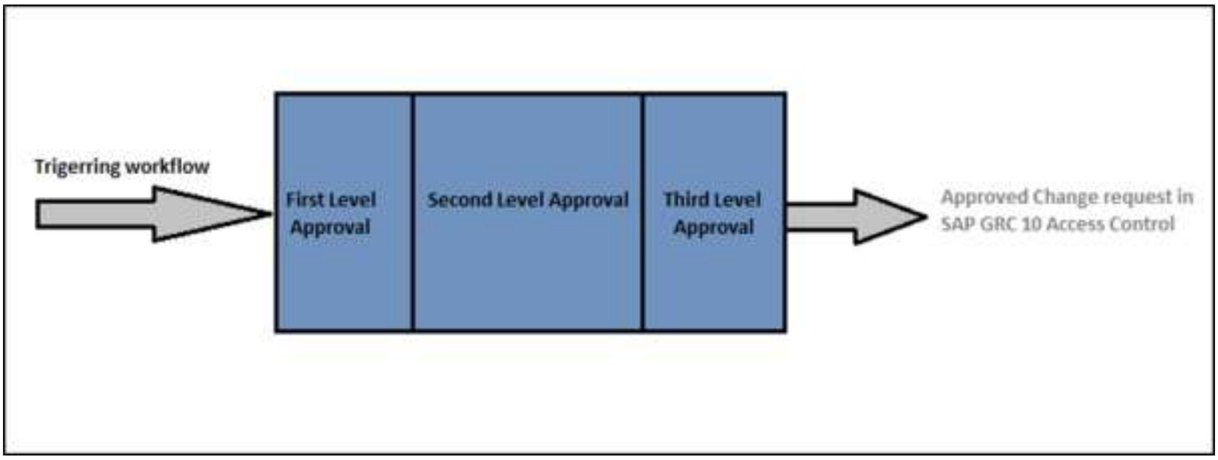
To use mitigation control at organization hierarchy, let us say you have performed risk analysis at organization level and the user violates all child organization rules and meets the condition of parent rule and only parent rule shows up; you can perform risk mitigation in the following ways:

- Mitigation on user level
- Mitigation on organization level

20. SAP GRC – Workflow Integration

In SAO GRC 10.0, a workflow is triggered in the following situations:

- To create or update risks.
- To create or update mitigation controls.
- To assign mitigation controls.



Activate workflow-based risk and control maintenance

As you follow workflow-based change management approach in risk analysis and remediation, you have to perform the following steps:

- Go to Configuration tab -> workflow options
- Set the below parameters:
- Set parameter Risk Maintenance to YES
- Set parameter Mitigation Control Maintenance to YES
- Set parameter Mitigation to YES
- Set up the Workflow Web Service URL:

  http://<server>:<port>/AEWFRequestSubmissionService_5_2/Config1?wsdl&style=document

- Customize the workflows need to be performed inside the Workflow Engine.

Workflow-based Risk and Control Maintenance

When you maintain a risk or a control is in SAP GRC, you perform the following steps:

Step 1: In Access Control, a workflow is triggered to perform a risk or a control workflow

Step 2: When you get the required approvals, approval steps depend on customer requirement.

Step 3: Get an audit trail documenting the complete approval process.

SAP GRC — Global Trade Services

Using SAP GRC Global Trade Services, you can improve cross-border supply chain of goods in an organization. This application allows you to automate the trade processes and helps you to control the cost and reduce the risk of penalties and also to manage inbound and outbound processes.

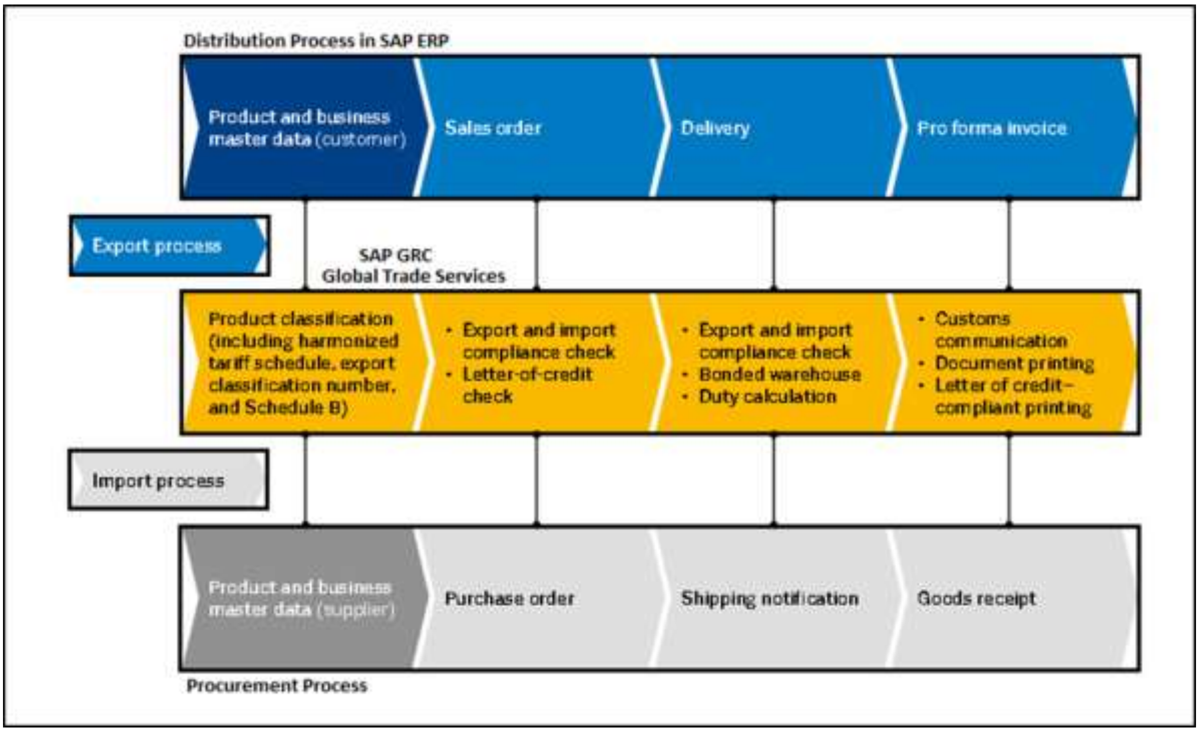
Using GTS, you can create **centralize single repository** that is used to contain all compliance master data and content.

The following are the key advantages of using Global Trade Services:

- It helps in reducing the cost and effort of managing compliance for global trading.
- It can ease time-consuming manual tasks and helps in improving productivity.
- Reduces the penalties for trade compliance violations
- It helps you to create and improve the brand and image and avoid trade with sanctioned or denied parties.
- Paves way for customer satisfaction and improves the quality of service.
- It fastens the inbound and outbound processes by performing customs clearance and also helps in removing unnecessary delays.

Integration between SAP ERP and SAP Global Trade Services

The following illustration shows the process flow of integration between SAP ERP and SAP Global Trade Services:


Distribution Process in SAP ERP
Product and business master data (customer)
Sales order
Delivery
Pro forma invoice
Export process
SAP GRC Global Trade Services
Product classification (including harmonized tariff schedule, export classification number, and Schedule B)
• Export and import compliance check
• Letter-of-credit check
• Export and import compliance check
• Bonded warehouse
• Duty calculation
• Customs communication
• Document printing
• Letter of credit–compliant printing
Import process
Product and business master data (supplier)
Purchase order
Shipping notification
Goods receipt
Procurement Process

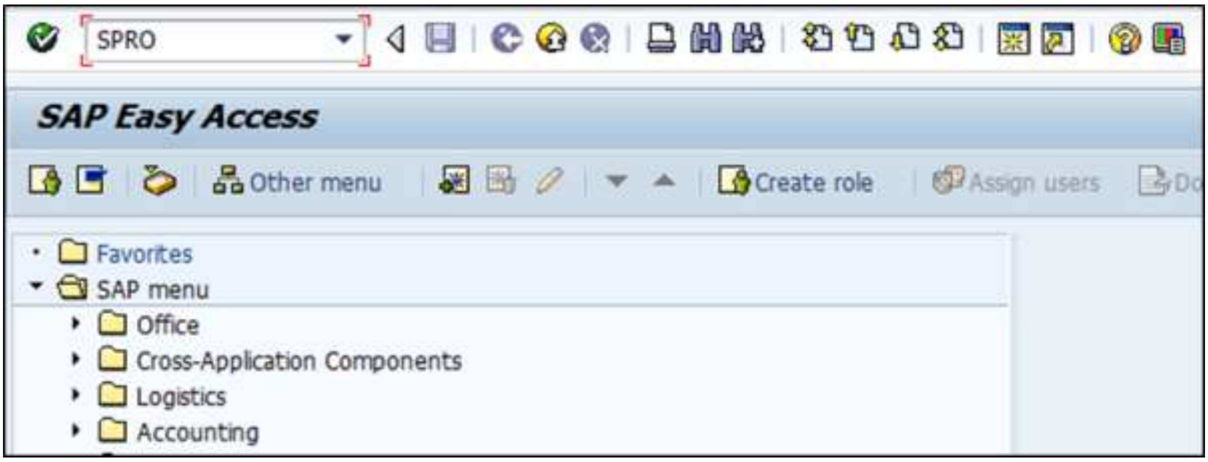
21. SAP GRC — Installation and Configuration

When you install SAP GRC, there are various configuration and settings that you need to perform in GRC. The key activities include:

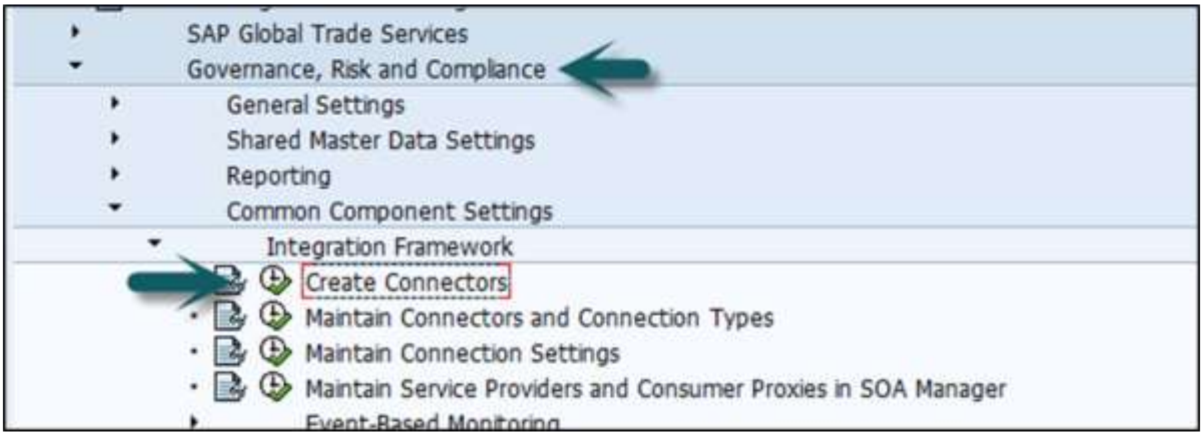
- Creating connectors in GRC
- Configuring AMF to use the connectors
- Creating callback connectors
- Creating connections in GRC is standard process of creating RFC connection using T-Code: SM59

SAP GRC is available in SAP Easy Access -> under Governance Risk Compliance folder.

Step 1: Open SAP Easy access menu and use T-Code: SPRO

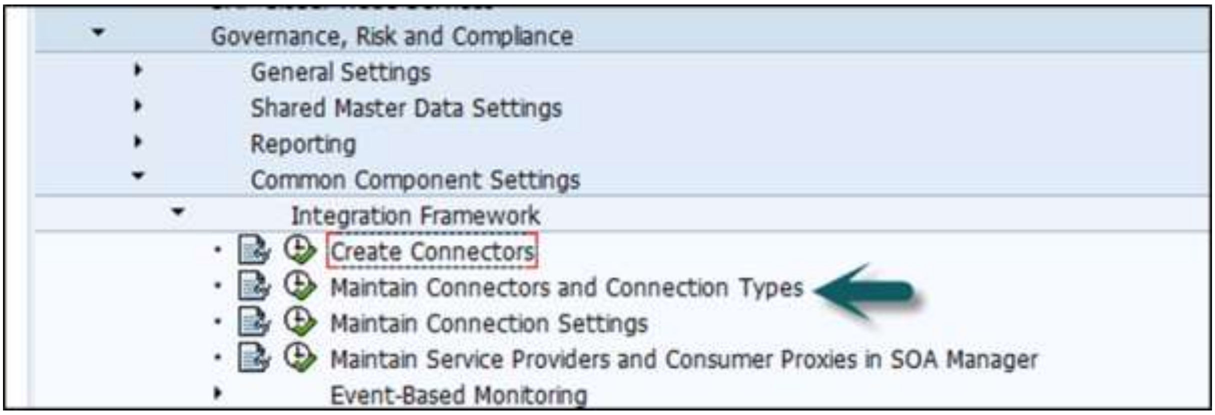


Step 2: Go to Governance, Risk and Compliance under SAP Reference IMG -> Common Component Settings -> Integration Framework -> Create Connectors


SAP Global Trade Services
Governance, Risk and Compliance
General Settings
Shared Master Data Settings
Reporting
Common Component Settings
Integration Framework
Create Connectors
Maintain Connectors and Connection Types
Maintain Connection Settings
Maintain Service Providers and Consumer Proxies in SOA Manager
Event-Based Monitoring

Step 3: Create connector is shortcut for creating SM59 connection.

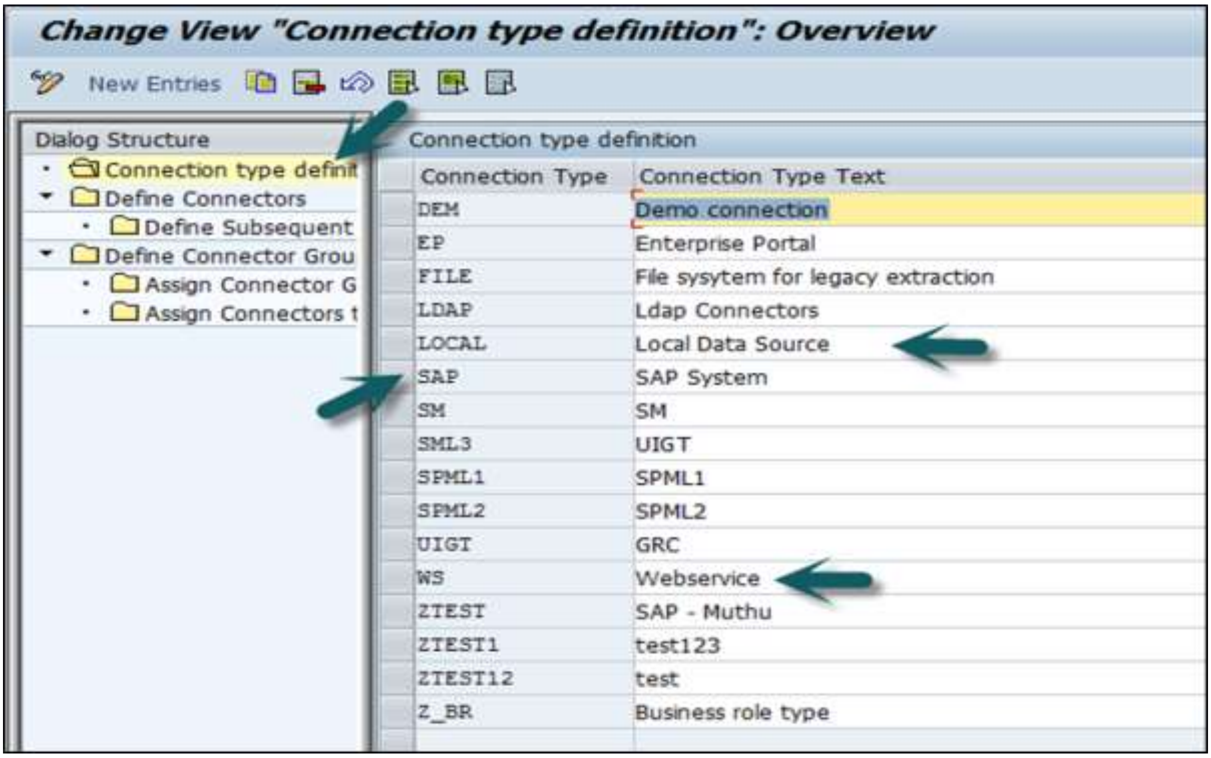
Step 4: To see existing connections, go to Maintain Connectors and Connection Types:


Governance, Risk and Compliance
General Settings
Shared Master Data Settings
Reporting
Common Component Settings
Integration Framework
Create Connectors
Maintain Connectors and Connection Types
Maintain Connection Settings
Maintain Service Providers and Consumer Proxies in SOA Manager
Event-Based Monitoring

You can see connector types as shown below. These connector types can be used for configuration for different purposes:

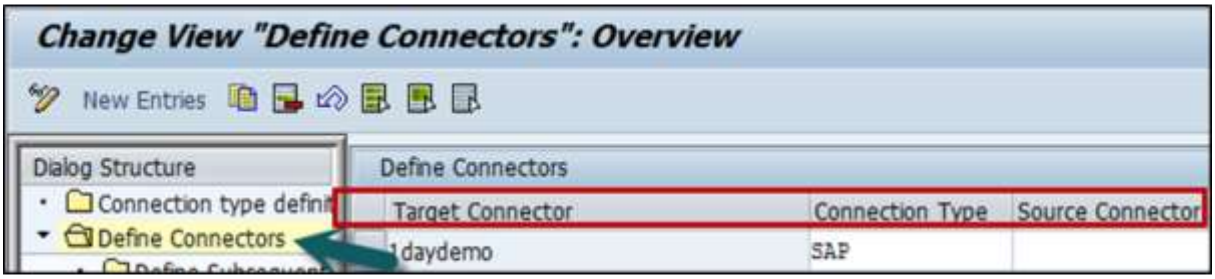
- Local system connectors are used to integrate with the SAP BusinessObjects Access Control application for monitoring segregation of duty violations
- Web service connectors are used for external partner data sources (see section
- SAP system connectors are used in all other cases.

Step 5: Go to **Connection Type Definition** tab:



Connection Type	Connection Type Text
DEM	Demo connection
EP	Enterprise Portal
FILE	File sysytem for legacy extraction
LDAP	Ldap Connectors
LOCAL	Local Data Source
SAP	SAP System
SM	SM
SML3	UIGT
SPML1	SPML1
SPML2	SPML2
UIGT	GRC
WS	Webservice
ZTEST	SAP - Muthu
ZTEST1	test123
ZTEST12	test
Z_BR	Business role type

Step 6: Define which of the connectors previously defined in SM59 can be used in monitoring. Go to define Connectors

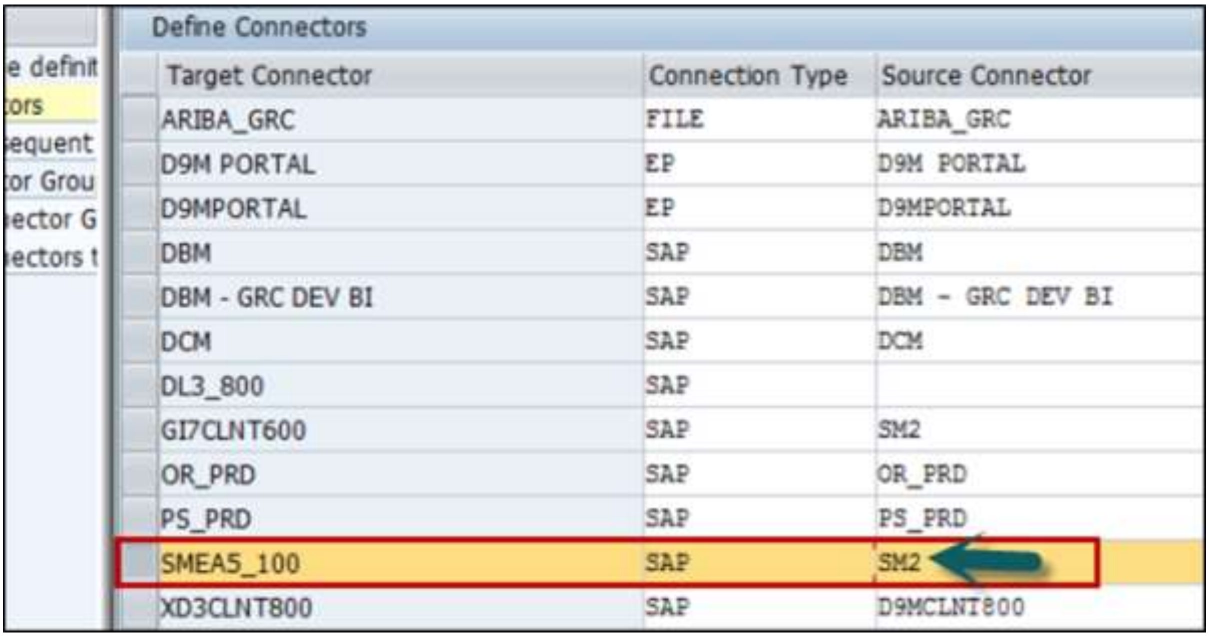


Change View "Define Connectors": Overview

Define Connectors

Target Connector	Connection Type	Source Connector
1daydemo	SAP	

Step 7: In the screen you can see a connector name — SMEA5_100. This is a connector which shows a connector to an ECC system.



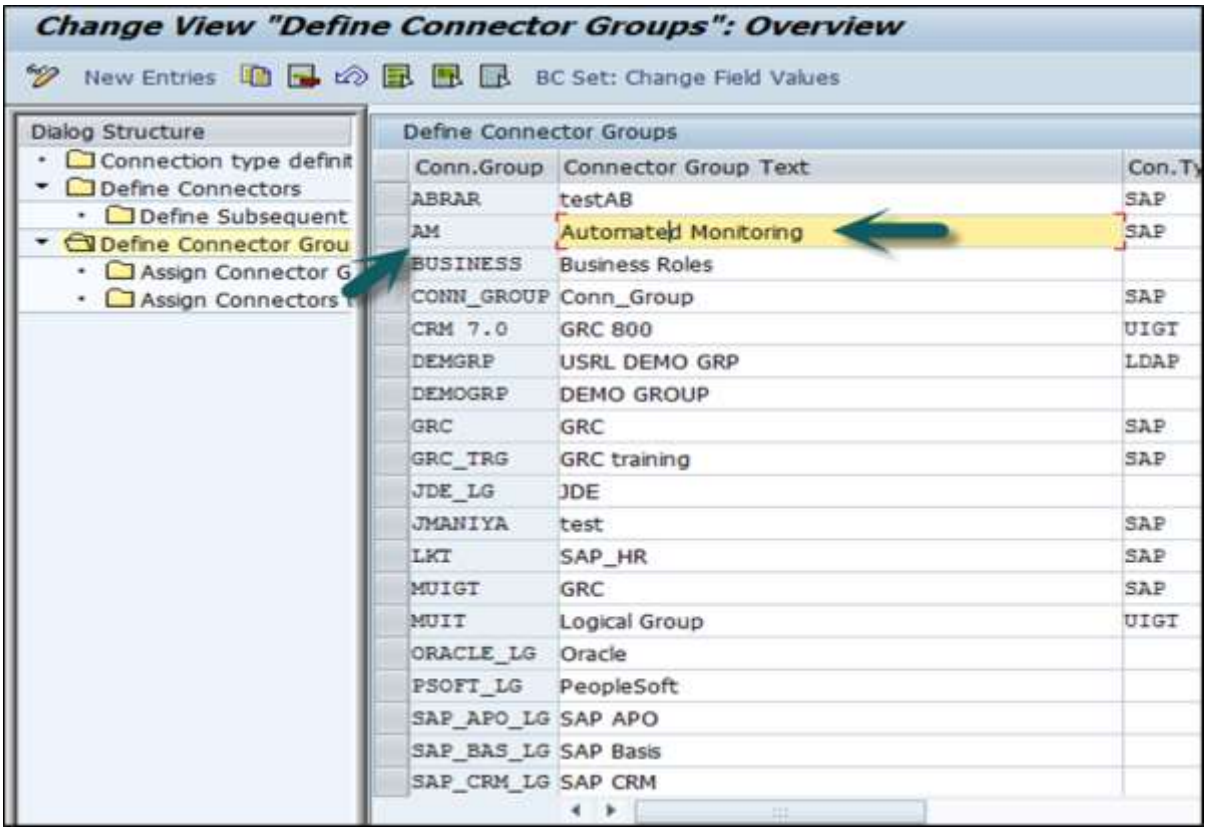
Define Connectors

Target Connector	Connection Type	Source Connector
ARIBA_GRC	FILE	ARIBA_GRC
D9M PORTAL	EP	D9M PORTAL
D9MPORTAL	EP	D9MPORTAL
DBM	SAP	DBM
DBM - GRC DEV BI	SAP	DBM - GRC DEV BI
DCM	SAP	DCM
DL3_800	SAP	
GI7CLNT600	SAP	SM2
OR_PRD	SAP	OR_PRD
PS_PRD	SAP	PS_PRD
SMEA5_100	SAP	SM2
XD3CLNT800	SAP	D9MCLNT800

The third column that lists the name of a connector which is defined in the monitored system, and which is configured to point back to the GRC system being configured here.

SMEA5_100 is another connector in the GRC system and it points to an ERP system which is to be monitored. SM2 is a connector on the ECC system and it points back to GRC system.

Step 8: Define Connector Group Screen on the left side.



Change View "Define Connector Groups": Overview

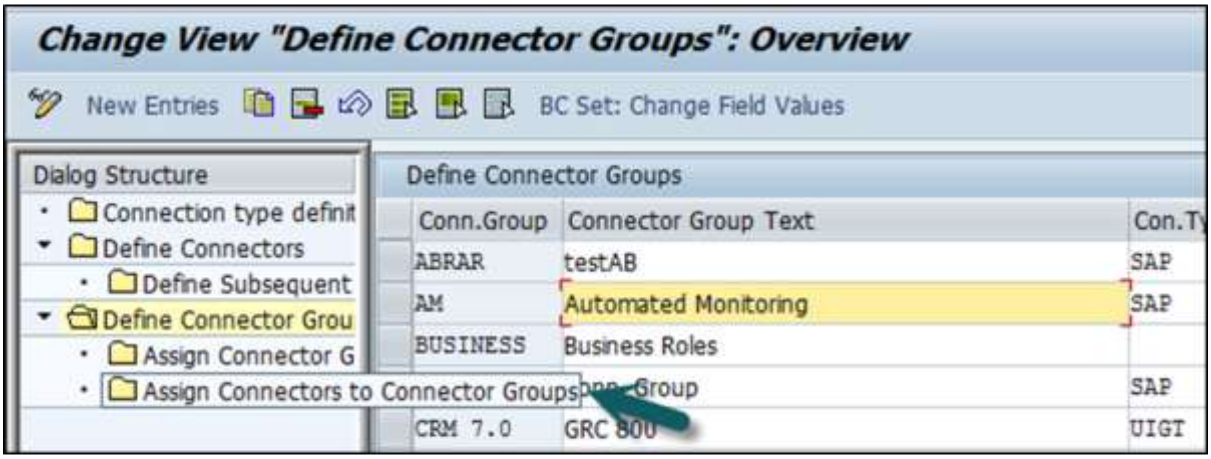
Dialog Structure
- Connection type definit
- Define Connectors
  - Define Subsequent
- Define Connector Grou
  - Assign Connector G
  - Assign Connectors t

Define Connector Groups

Conn.Group	Connector Group Text	Con.Ty
ABRAR	testAB	SAP
AM	Automated Monitoring	SAP
BUSINESS	Business Roles	
CONN_GROUP	Conn_Group	SAP
CRM 7.0	GRC 800	UIGT
DEMGRP	USRL DEMO GRP	LDAP
DEMOGRP	DEMO GROUP	
GRC	GRC	SAP
GRC_TRG	GRC training	SAP
JDE_LG	JDE	
JMANIYA	test	SAP
LKT	SAP_HR	SAP
MUIGT	GRC	SAP
MUIT	Logical Group	UIGT
ORACLE_LG	Oracle	
PSOFT_LG	PeopleSoft	
SAP_APO_LG	SAP APO	
SAP_BAS_LG	SAP Basis	
SAP_CRM_LG	SAP CRM	

Step 9: Here you have to ensure that all the connector configurations for automated monitoring should belong to the configuration group called **Automated Monitoring** as shown above under **define automated monitoring connector group**.

Step 10: Go to **assign connectors to connector group** on the left side.



Change View "Define Connector Groups": Overview

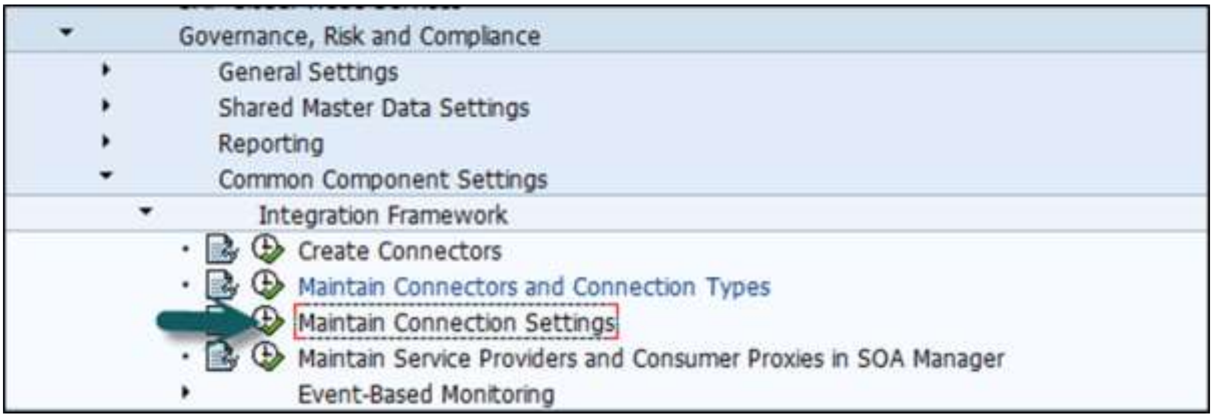
Dialog Structure
- Connection type definit
- Define Connectors
  - Define Subsequent
- Define Connector Grou
  - Assign Connector G
  - Assign Connectors to Connector Groups

Define Connector Groups

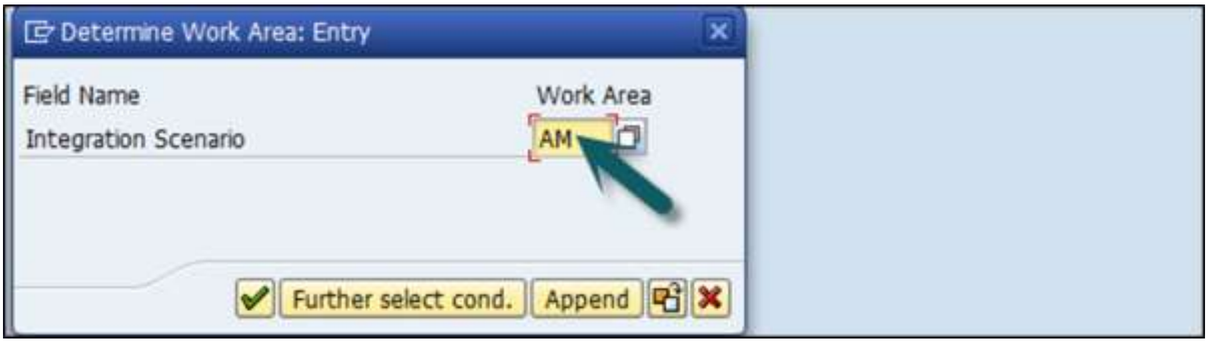
Conn.Group	Connector Group Text	Con.Ty
ABRAR	testAB	SAP
AM	Automated Monitoring	SAP
BUSINESS	Business Roles	
	Conn_Group	SAP
CRM 7.0	GRC 800	UIGT

Step 11: Assign the connector to AM connector group as mentioned in the above screenshot.

Step 12: Go to **Maintain Connection Settings** in main menu as in the following screenshot.

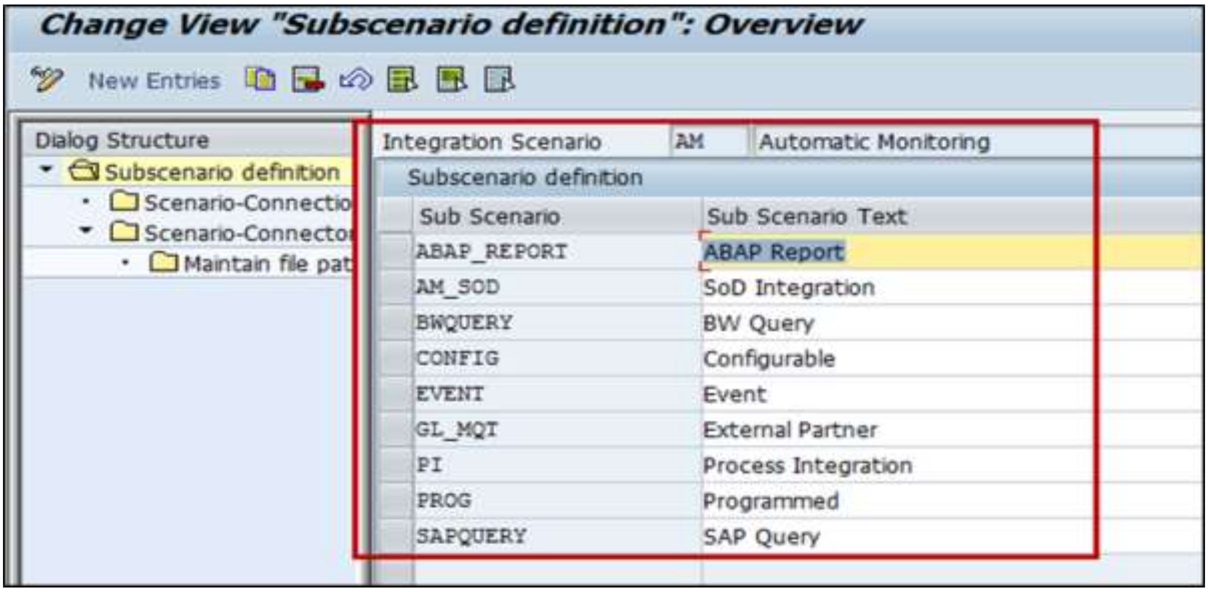

Governance, Risk and Compliance
General Settings
Shared Master Data Settings
Reporting
Common Component Settings
Integration Framework
Create Connectors
Maintain Connectors and Connection Types
Maintain Connection Settings
Maintain Service Providers and Consumer Proxies in SOA Manager
Event-Based Monitoring

Step 13: You need to enter the integration scenario you want, enter AM as in the following screenshot:



Field Name	Work Area
Integration Scenario	AM

Step 14: Click on the green tick mark as shown in the above screenshot; you will be directed to the following screen with nine sub-scenarios.



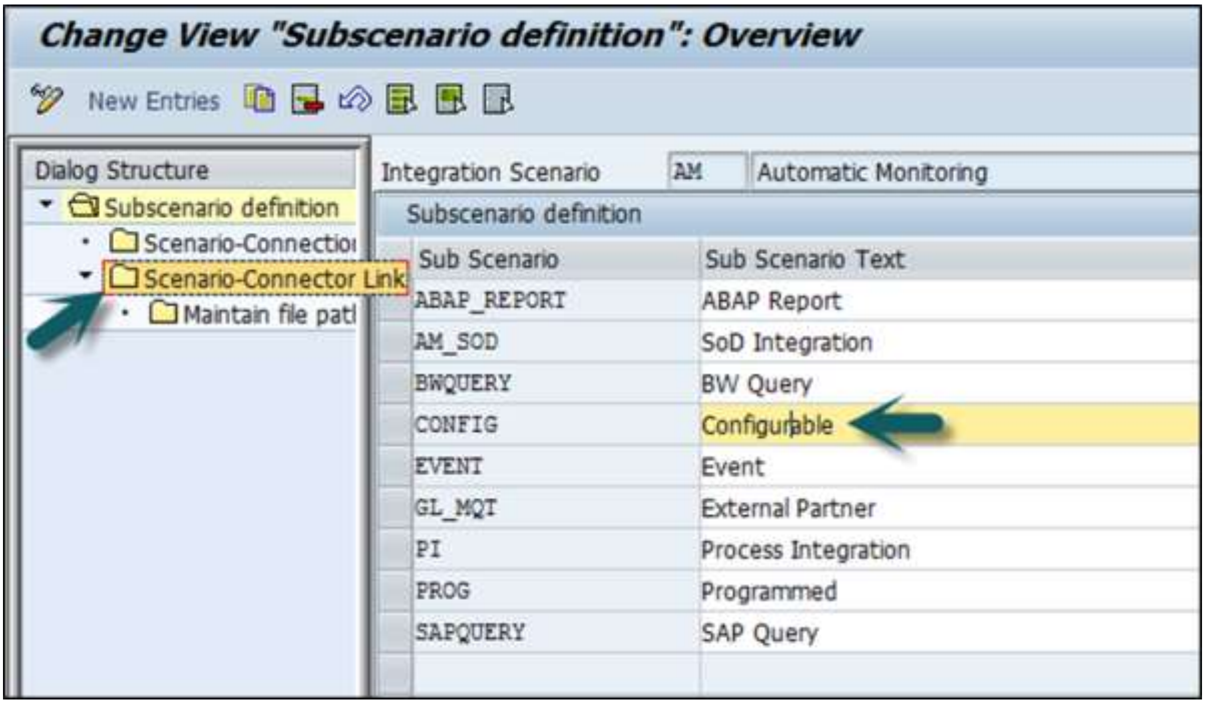
Integration Scenario AM Automatic Monitoring

Sub Scenario	Sub Scenario Text
ABAP_REPORT	ABAP Report
AM_SOD	SoD Integration
BWQUERY	BW Query
CONFIG	Configurable
EVENT	Event
GL_MQT	External Partner
PI	Process Integration
PROG	Programmed
SAPQUERY	SAP Query

The highlighted box shows nine entries called sub-scenarios and they represent the different types of data sources and business rules supported under Process Control 10.

Step 15: For the System to be monitored, you need to link the corresponding connector to that sub-scenario.

Step 16: Select the sub-scenario you want configurable and then choose Scenario Connector Link in the left side as shown below:



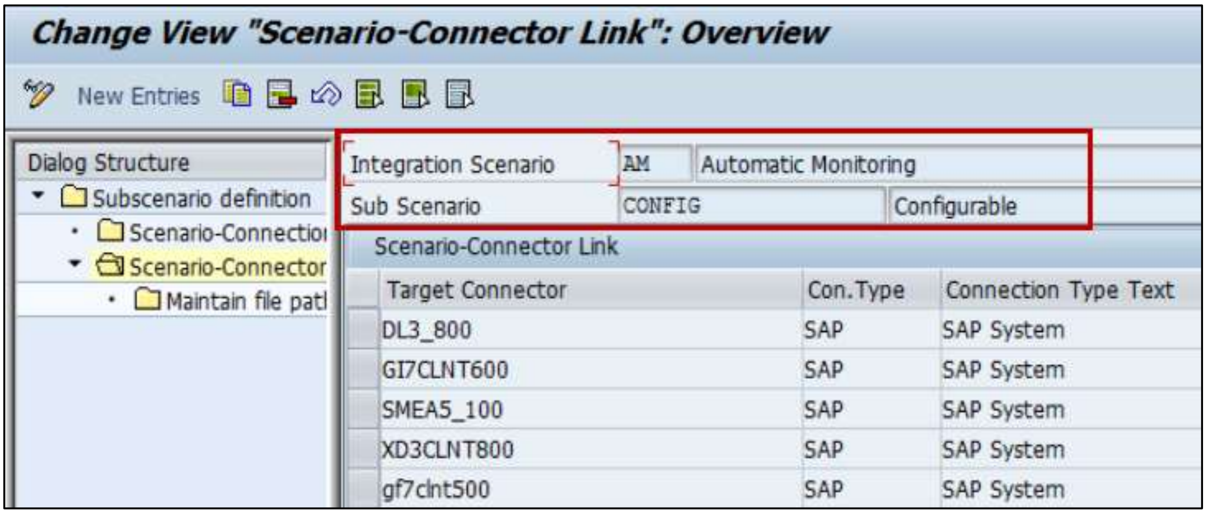
Change View "Subscenario definition": Overview

Integration Scenario AM Automatic Monitoring

Subscenario definition

Sub Scenario	Sub Scenario Text
ABAP_REPORT	ABAP Report
AM_SOD	SoD Integration
BWQUERY	BW Query
CONFIG	Configurable
EVENT	Event
GL_MQT	External Partner
PI	Process Integration
PROG	Programmed
SAPQUERY	SAP Query

Step 17: You will be directed to the following screen:



Change View "Scenario-Connector Link": Overview

Integration Scenario AM Automatic Monitoring

Sub Scenario CONFIG Configurable

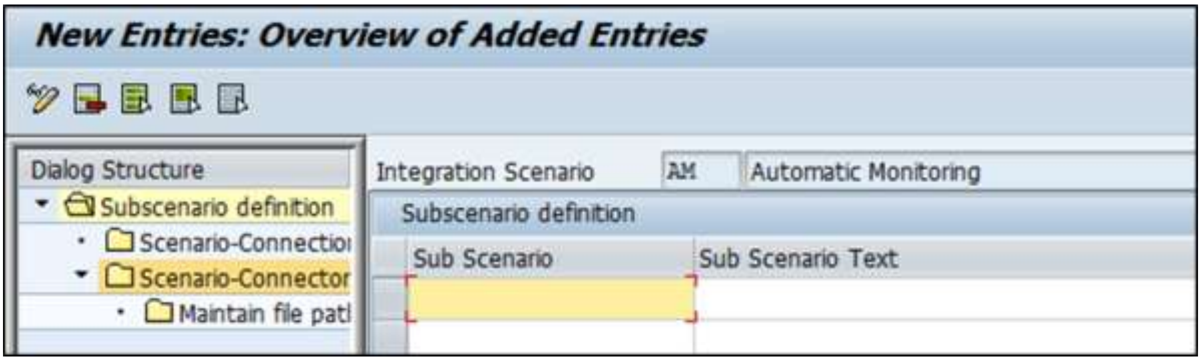
Scenario-Connector Link

Target Connector	Con.Type	Connection Type Text
DL3_800	SAP	SAP System
GI7CLNT600	SAP	SAP System
SMEA5_100	SAP	SAP System
XD3CLNT800	SAP	SAP System
gf7clnt500	SAP	SAP System

Step 18: Now the connector you want to use for that scenario is not already in the list for that sub-scenario,

- You can click on New Entries button at the top to add it.

- You can follow these recommendations to add subscenarios:
  - ABAP Applications: ABAP report, SAP query, configurable program
  - SAP BW: BW query
  - Non SAP System: External Partner
  - Process Integrator: PI
  - GRC System: SoD integration

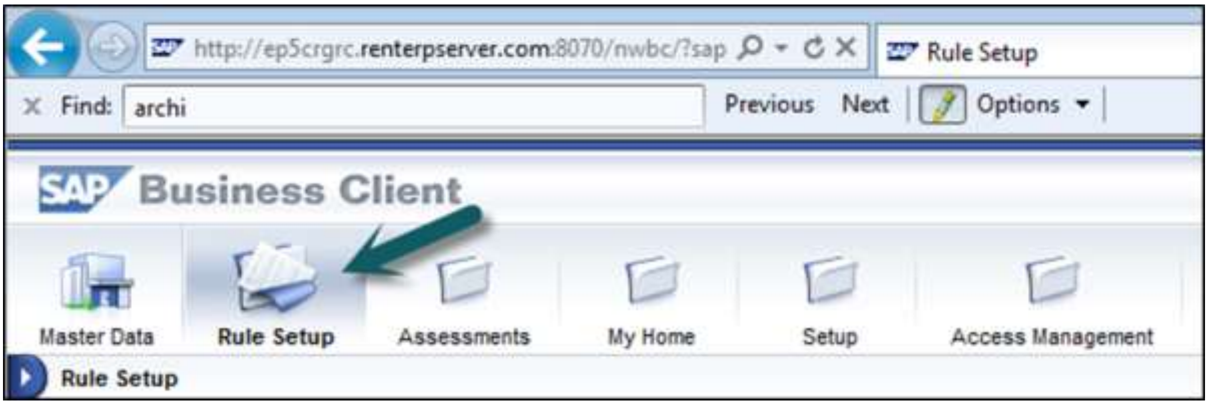


New Entries: Overview of Added Entries

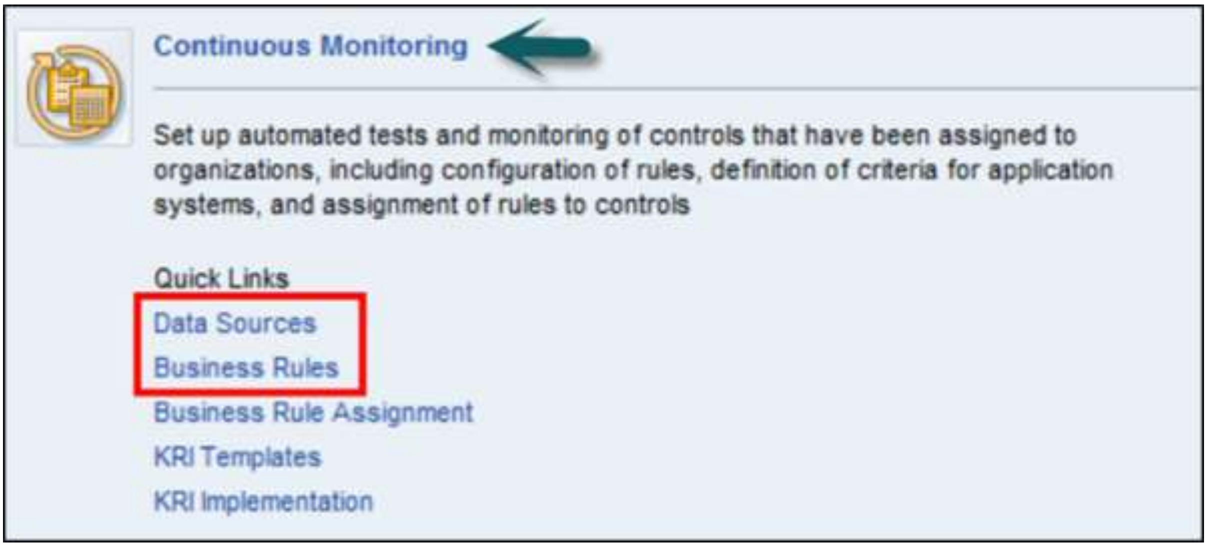
Integration Scenario AM Automatic Monitoring

22. SAP GRC — Data Sources and Business Rules

In SAP GRC Process Control, you can create data sources. Here, the design time user interfaces are under Rule Setup option in Business client.



Go to continuous monitoring section where you can find **Data Sources** and **Business Rules** option.



Continuous Monitoring

Set up automated tests and monitoring of controls that have been assigned to organizations, including configuration of rules, definition of criteria for application systems, and assignment of rules to controls

Quick Links

Data Sources

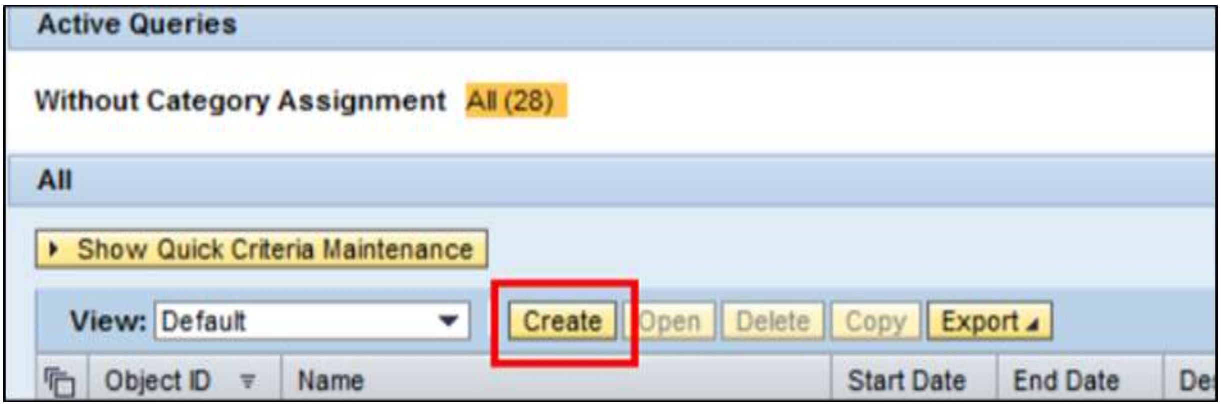
Business Rules

Business Rule Assignment

KRI Templates

KRI Implementation

To create a new Data Source, click on Data Sources -> Create.

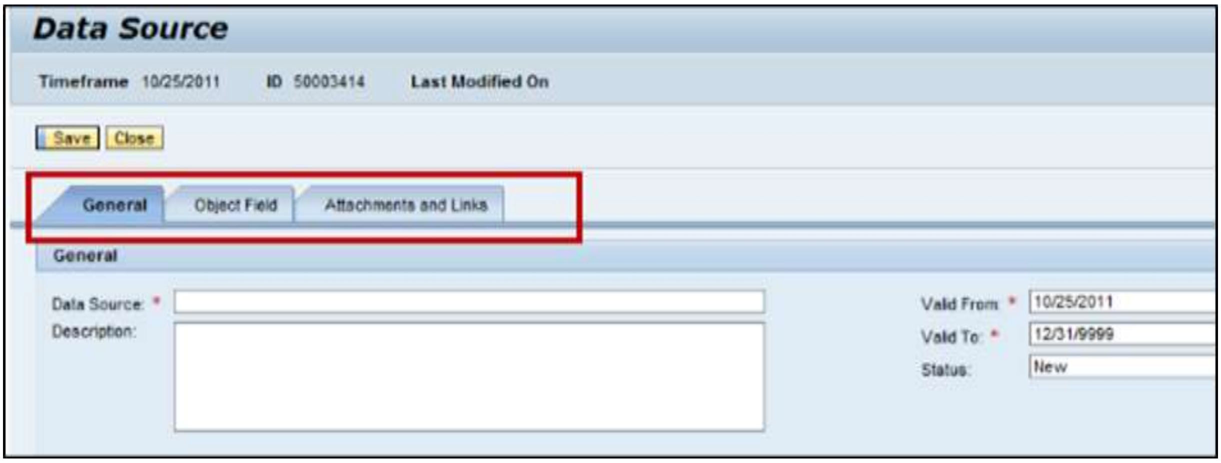


In the next field, you can see three different tabs to define the data source.

- General Tab
- Object Field
- Link and Attachment

In General tab, enter the following details:

- Name of data source
- Start date of the validity period
- End date of the validity period
- Status



Timeframe 10/25/2011 ID 50003414 Last Modified On

Data Source: *

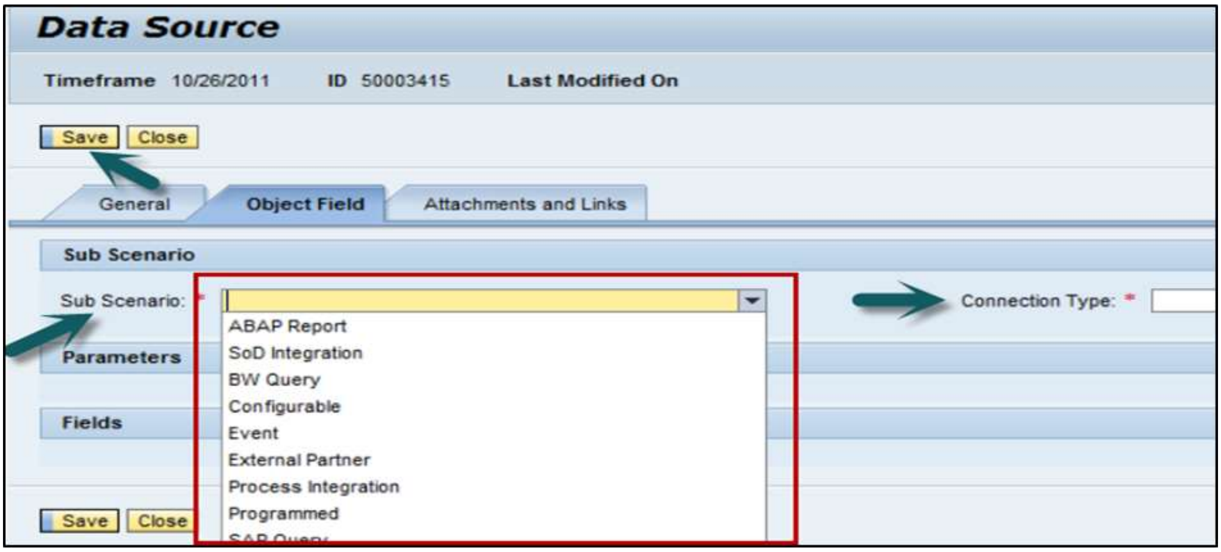
Description:

Valid From: * 10/25/2011

Valid To: * 12/31/9999

Status: New

Go to **Object Field** tab, select the following fields:

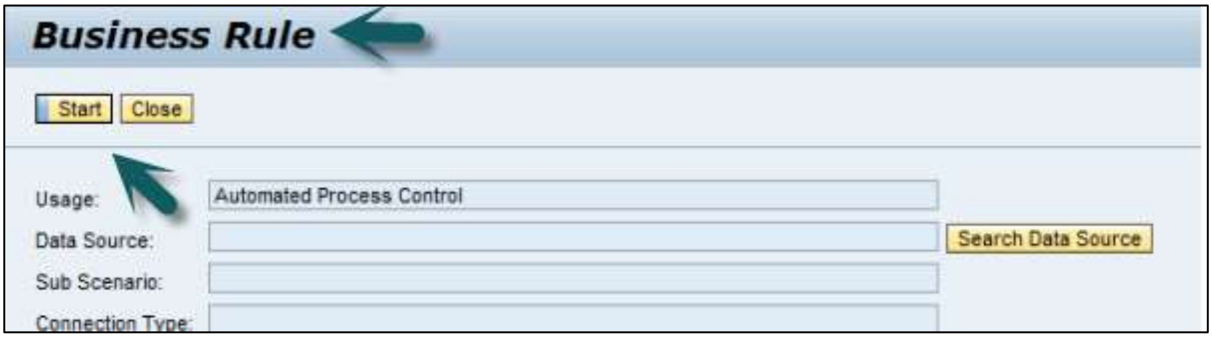


23. SAP GRC — Creating Business Rules

In SAP GRC 10.0, you can use Business Rules to filter the data stream that is coming from the data sources and you can apply the user configured conditions/calculations against that data to determine if there is a problem which requires attention.

The Business Rule type purely depends on the Data Source type.

Go to Business Rules under Rule Setup.



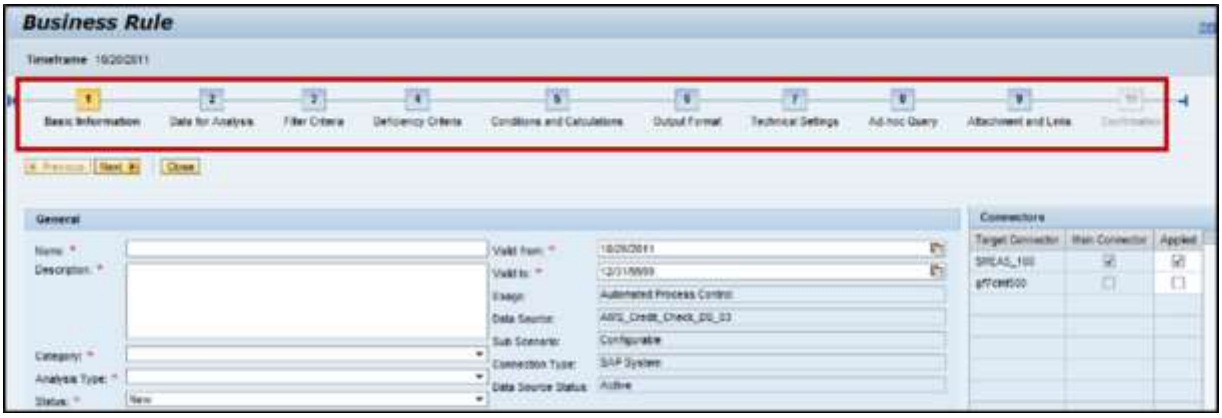
Usage: Automated Process Control

Data Source:

Sub Scenario:

Connection Type:

To create new business rules, there is a list of steps that you need to follow with few of the Data Source types.



Timeframe 10/20/2011

Name: *

Description: *

Category: *

Analysis Type: *

Status: * New

Valid from: * 10/20/2011

Valid to: * 12/31/9999

Usage: Automated Process Control

Data Source: ARS_Credit_Check_DS_03

Sub Scenario: Configurable

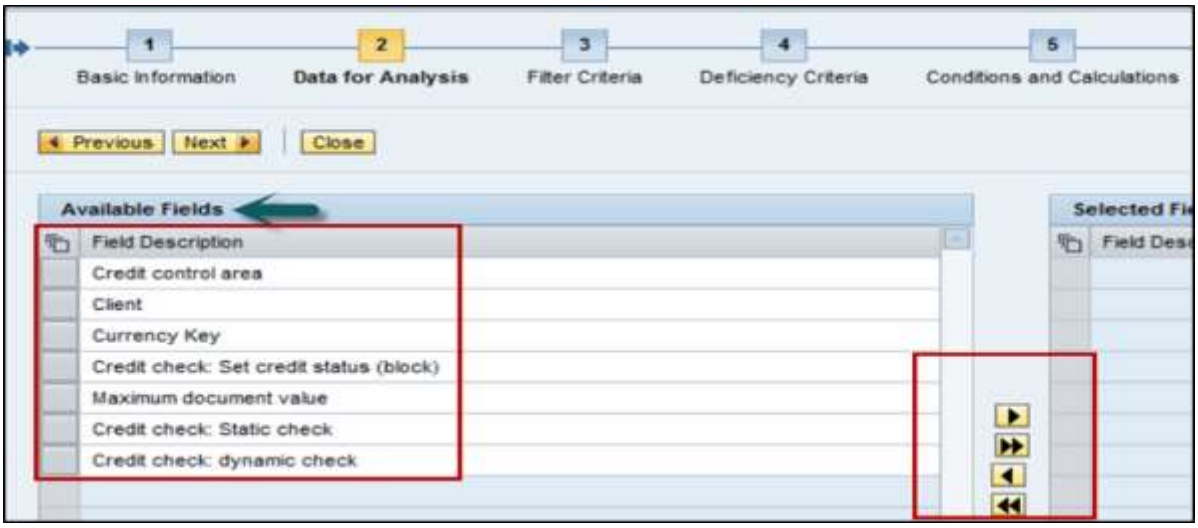
Connection Type: SAP System

Data Source Status: Active

Target Connector	Main Connector	Applied
SREAS_100	☑	☑
gf7clnt500	□	□

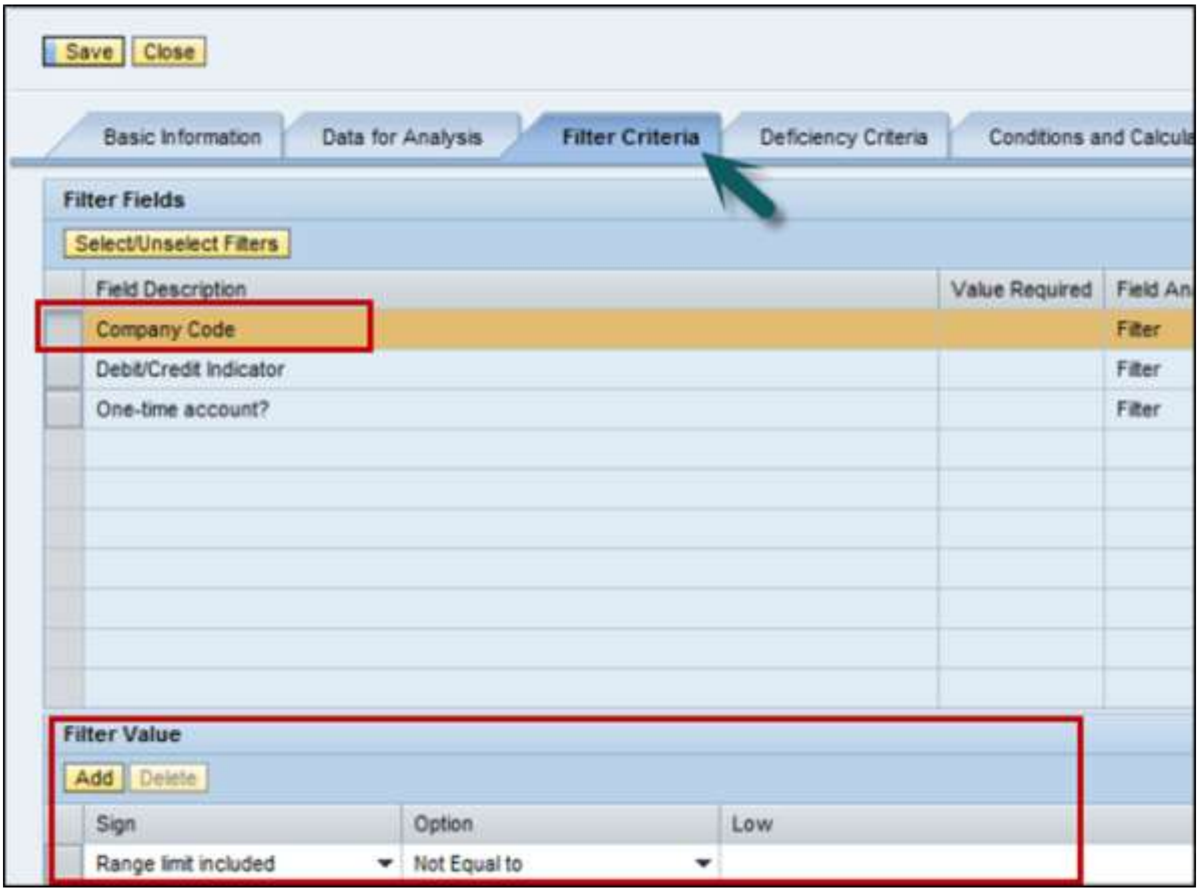
You need to define details in each tab. For example, in the **General** tab, you need to enter the basic information about business rule. **Business rule gives you data to filter the deficiencies**.

In Data for Analysis tab, you will see a list of available fields.



Field Description
Credit control area
Client
Currency Key
Credit check: Set credit status (block)
Maximum document value
Credit check: Static check
Credit check: dynamic check

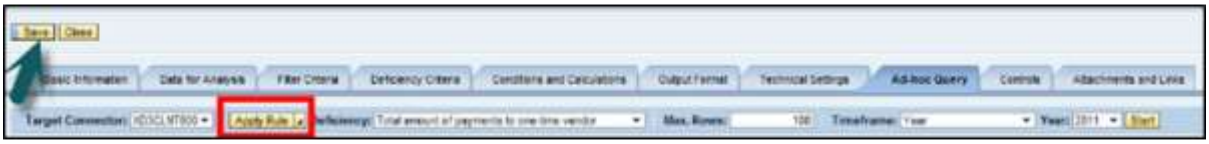
Go to filter criterial to pass the filter condition on available objects. You can select from different operators.



Field Description	Value Required	Field An
Company Code		Filter
Debit/Credit Indicator		Filter
One-time account?		Filter

Sign	Option	Low
Range limit included	Not Equal to	

When you define all the steps, you have an option to save the rule. If you want to apply the rule to Process Control, you can do by clicking **Apply** button.



Target Connection: XD3CLNT800

Deficiency: Total amount of payments to one-time vendor

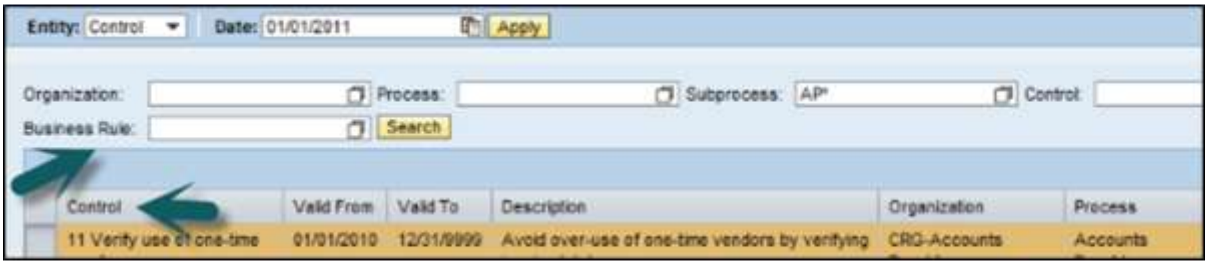
Max. Rows: 100

Timeframe: Year

Year: 2011

To assign business rule to a process control, go to Business rule assignment under Continuous Monitoring in Rule Setup.

Select the control and search for the Business rule to apply.



Entity: Control

Date: 01/01/2011

Organization:

Process:

Subprocess: AP*

Control:

Business Rule:

Control	Valid From	Valid To	Description	Organization	Process
11 Verify use of one-time	01/01/2010	12/31/9999	Avoid over-use of one-time vendors by verifying	CRG-Accounts	Accounts

We have now understood how to create Data Sources and Business Rules to apply filter on Data Sources and how to assign business rules to process controls.