

# SAP GRC How-to Guide: Performing Risk Analysis with Enterprise Portal Roles



## Applies to:

This document applies to Risk Analysis and Remediation capability of SAP GRC Access Controls Suite 5.3. For more information, visit the [Governance, Risk, and Compliance homepage](#).

## Summary

This document will enable the implementation partners and implementers to configure the Rules and perform Risk Analysis on the Enterprise Portal Roles. This guide will also discuss about all the steps which are required to achieve analysis of Enterprise Portal and seek as well as remove SoD Violations from the Enterprise Portal Environment.

**Author:** Aman Chuttani

**Company:** SAP

**Created on:** 28 July 2008

## Author Bio

Aman Chuttani works as a consultant in SAP's GRC RIG. He has gained extensive experience supporting SAP's customers in the implementation of SAP GRC Access Controls.

## Table of Contents

Downloading Enterprise Portal Objects .....	3
Creating Enterprise Portal Connector in RAR Application .....	6
Upload Authorization Objects for EP System .....	7
Defining SoD Rules for the EP System .....	8
Define Function .....	8
Define Risk.....	10
Generate Rules Individually .....	11
Mass Generation of Rules.....	12
Related Content.....	13
Copyright.....	14

## Downloading Enterprise Portal Objects

The EPRTA enables the administrator to download the authorization objects for EP system. These objects will be used to define the SoD Rules for the EP system. In order to download the auth. Objects for EP system we need to follow the following procedure.

1. Log-in to SAP NetWeaver Web Service Navigator on the EP system with following link.  
<http://<server-id>:<port-id>/wsnavigator/enterwsdl.html>
2. If the EPRTA has been successfully installed on the system, you can find the “**CCRTAWS**” on the main page of Web Service Navigator

**SAP** THE BEST-RUN BUSINESSES RUN SAP

### Web Services Navigator

*Welcome to the Web Services Navigator*

Enter the WSDL URL of the Web service:

Available Web Services - Cluster Node 305522250

- + AEWFCADApproversServiceWS\_5\_2
- + AEWExitServiceWS\_5\_2
- + AEWRequestSubmissionService\_5\_2
- + **CCRTAWS** → Enterprise Portal RTA Web Service
- + CMSRTS
- + ConfigurationWS
- + GRMGWSTest

3. Open the Web Service in Test Mode. You can find the method “**getMasterData**” in the Web Service.



THE BEST-RUN BUSINESSES RUN SAP

Home

Overview

WSDLs

Test

## CCRTAWS

### Test

Config1Port\_Document

#### Operations

<b>getDeletedRoles</b> (test.types.p3.GetDeletedRoles parameters)
<b>getDeletedUsers</b> (test.types.p3.GetDeletedUsers parameters)
<b>getMasterData</b> (test.types.p3.GetMasterData parameters)
<b>getMenuAction</b> (test.types.p3.GetMenuAction parameters)
<b>getMenuPermission</b> (test.types.p3.GetMenuPermission parameters)
<b>getMenuSync</b> (test.types.p3.GetMenuSync parameters)
<b>getRoleAction</b> (test.types.p3.GetRoleAction parameters)
<b>getRolePermission</b> (test.types.p3.GetRolePermission parameters)
<b>getRoleSync</b> (test.types.p3.GetRoleSync parameters)
<b>getUserAction</b> (test.types.p3.GetUserAction parameters)
<b>getUserOrg</b> (test.types.p3.GetUserOrg parameters)
<b>getUserPermission</b> (test.types.p3.GetUserPermission parameters)
<b>getUserRoles</b> (test.types.p3.GetUserRoles parameters)
<b>getUserSync</b> (test.types.p3.GetUserSync parameters)
<b>login</b> (test.types.p3.Login parameters)
<b>logout</b> (test.types.p3.Logout parameters)

- Click the method. You can now provide the path on the server where the file needs to be downloaded.

**Note:** The file will be only downloaded on the server location.



Home Overview WSDLs Test

getMasterData

- parameters (test.types.p3.GetMasterData)
  - fileDto (test.types.FileInputDto)  NULL
  - filePath (String) C:\EP\_Master\_Data.txt  SKIP

Timeout (seconds):

- Once successful completion of the process the message would be displayed on the web-page.



Home Overview WSDLs Test

**Request**

getMasterData

- parameters (test.types.p3.GetMasterData)
  - fileDto (test.types.FileInputDto)
  - filePath (String) C:\EP\_Master\_Data.txt

```
POST /CCRTAWS/Config1?style=document HTTP/1.1
Host: localhost:53000
Content-Type: text/xml; charset=UTF-8
Connection: close
Cookie: <value is hidden>
Cookie: <value is hidden>
Content-Length: 468
SOAPAction: ""

<?xml version="1.0" encoding="UTF-8" ?><
```

Wrap/Unwrap

**Response**

getMasterData

- response (test.types.p3.GetMasterDataResponse)
  - Response (String) File imported successfully

```
HTTP/1.1 200 OK
Connection: close
Server: SAP J2EE Engine/7.00
Content-Type: text/xml; charset=UTF-8
Date: Tue, 14 Oct 2008 07:19:14 GMT

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http:
```

Wrap/Unwrap

## Creating Enterprise Portal Connector in RAR Application

In order to connect GRC application to the enterprise portal, we need to create connector in RAR application. To create a connector we need to follow the following steps:

1. Log-in to the RAR application with following link as application administrator

<http://<server-id>:<port-id>/webdynpro/dispatcher/sap.com/grc-ccappcomp/ComplianceCalibrator>

2. Go to Configuration Tab.
3. Select Connector -> Create
4. Enter the following details for the connector and click Save button

Field	Value
System	Enterprise System ID in the landscape which will be referred through-out the application
System Name	Description of the EP system being connected
System Type	Portal
Connection Type	Web Service
URL	URL of the RTA installed on the EP system. <a href="http://&lt;server-id&gt;:&lt;port-id&gt;/CCTRAWS/Config1?style=document">http://&lt;server-id&gt;:&lt;port-id&gt;/CCTRAWS/Config1?style=document</a>
User ID, Password	User Credentials to access the EP system
Server Name	<server-id>
Port Number	<port-id>

The screenshot displays the SAP GRC Access Control Risk Analysis and Remediation interface. The top navigation bar includes the SAP logo, the title 'SAP GRC Access Control Risk Analysis and Remediation', the user name 'Welcome Aman Chuttani', and links for 'Help', 'About', and 'Logoff'. The main navigation tabs are 'Informer', 'Rule Architect', 'Mitigation', 'Alert Monitor', and 'Configuration'. The left sidebar shows a tree view of the application structure, with 'Connectors' expanded to show 'Create' and 'Search' options. The main content area is titled 'Change Connector' and contains the following fields:

- System: \* (Text input: LCL)
- System Name: \* (Text input: LocalHost)
- System Type: (Dropdown menu: Portal)
- Connection Type: (Dropdown menu: Web Service)
- URL: \* (Text input: http://localhost:53000/CCTRAWS)
- User ID: \* (Text input: sapgrc)
- Password: \* (Text input: masked with dots)
- Server Name: \* (Text input: localhost)
- Port Number: \* (Text input: 53000)

A 'Save' button is located at the bottom of the form.

## Upload Authorization Objects for EP System

The authorization objects downloaded from the EP system should be uploaded to the GRC RAR application in order to define SoD Rules for the EP System. To upload auth. objects we need to perform following steps:

1. Log-in to the RAR application with following link as application administrator  
<http://<server-id>:<port-id>/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCalibrator>
2. Go to Configuration Tab.
3. Select Upload Objects -> Text Objects.
4. Select the System Description of the EP system from the drop down menu.
5. Browse the authorization object file alias Master Data file (downloaded with help of RTA) as a local file or provide the server location where the file has been stored.
6. Click Foreground.
7. Once successfully uploaded, message would be displayed at the bottom of the screen.

The screenshot displays the SAP GRC Access Control interface. The top navigation bar includes the SAP logo, 'SAP GRC Access Control Risk Analysis and Remediation', and a user welcome message 'Welcome Aman Chuttani'. The main menu on the left is expanded to 'Upload Objects' > 'Text Objects'. The central panel, titled 'Text Objects Upload', contains a 'System' dropdown menu set to 'LocalHost', and two empty input fields for 'Local File' and 'Server File'. Below these fields are three buttons: 'Foreground' (highlighted), 'Background', and 'Cancel'. At the bottom of the interface, a green message bar states 'Upload text successfully executed'.

## Defining SoD Rules for the EP System

In order to generate SoD Rules for EP we need to:

1. Define Functions with non conflicting actions and permissions.
2. Define Risks with Functions having conflicting actions and permissions.
3. Generate Rules.

### Define Function

1. Log-in to the RAR application with following link as business process owner.  
<http://<server-id>:<port-id>/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCalibrator>
2. Go to Rule Architect Tab.
3. Go to Functions -> Create.
4. Define **Function ID, Description, Business process and Analysis Scope** for the function.
5. Define Actions for the Function.

The screenshot displays the SAP GRC Access Control interface. The main window is titled "Change Function" and contains the following fields:

- Function ID: EP01
- Description: EP Test 1
- Business Process: Basis
- Analysis Scope: Single System

Below these fields is a table for defining actions. The table has columns for System, Action, Description, and Status. A search dialog is open, showing a search for "\*GRC\*" in the Action field. The search results table is as follows:

Action	Description
pcd.portal_content/com.sap.grc.GRC0001/GRC0002	
pcd.portal_content/com.sap.grc.GRC0001/com.sap.test.IView0001	
pcd.portal_content/com.sap.grc.GRC0001/com.sap.grc.EP0001/com.sap.test.IView0001	
pcd.portal_content/com.sap.grc.GRC0001/com.sap.grc.EP0001/GRC0002	



## 6. Define Permissions for the Function.

The screenshot displays the SAP GRC Access Control interface. The main window is titled "Change Function" and shows details for function ID "EP01". The description is "EP Test 1", the business process is "Basis", and the analysis scope is "Single System". The "Permissions" tab is active, showing a list of permissions. A "Permission Definition" dialog is open, allowing the user to define a permission. The dialog fields are: Permission: pcd:portal\_content/com.sa, Field: PERM, Value From: FullControl, Value To: (empty), Search Type: (dropdown), and Status: Enable. Buttons for Save, Clear, and Cancel are visible at the bottom of the dialog.

## 7. Click Save.

**Note:** We need to provide **COMPLETE** pcd location for the actions or permissions which are being defined during this process. For instance, in the figure below, iView0001 can be accessed through a role with id "EP0001", hence we need to provide complete details of the iView0001 from where it can be accessed if it is required to be monitored under SoD Violations.

## Define Risk

1. Log-in to the RAR application with following link as business process owner.  
<http://<server-id>:<port-id>/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCalibrator>
2. Go to Rule Architect Tab.
3. Go to Risks -> Create.
4. Define **Risk ID, Description, Risk Type, Risk Level, Business Process and Status of the risk.**
5. As per requirements also define, **Detailed Description, Control Objective, Risk Owners, Rule Sets (to which this Risks should be included).**
6. Select the Conflicting functions from the “**Conflicting Functions**” Tab.

The screenshot displays the SAP GRC Access Control 'Edit Risk' screen. The top navigation bar includes the SAP logo, 'SAP GRC Access Control Risk Analysis and Remediation', and a user welcome message for Aman Chuttani. The main interface is divided into a left-hand navigation menu and a central workspace. The workspace is titled 'Edit Risk' and contains a form with the following fields:

- Risk ID: \* (Text input: EPR1)
- Description: \* (Text input: EP Test Risk 1)
- Risk Type: (Dropdown menu: Segregation of Duties)
- Risk Level: (Dropdown menu: Medium)
- Business Process: (Dropdown menu: Basis)
- Status: (Dropdown menu: Enable)

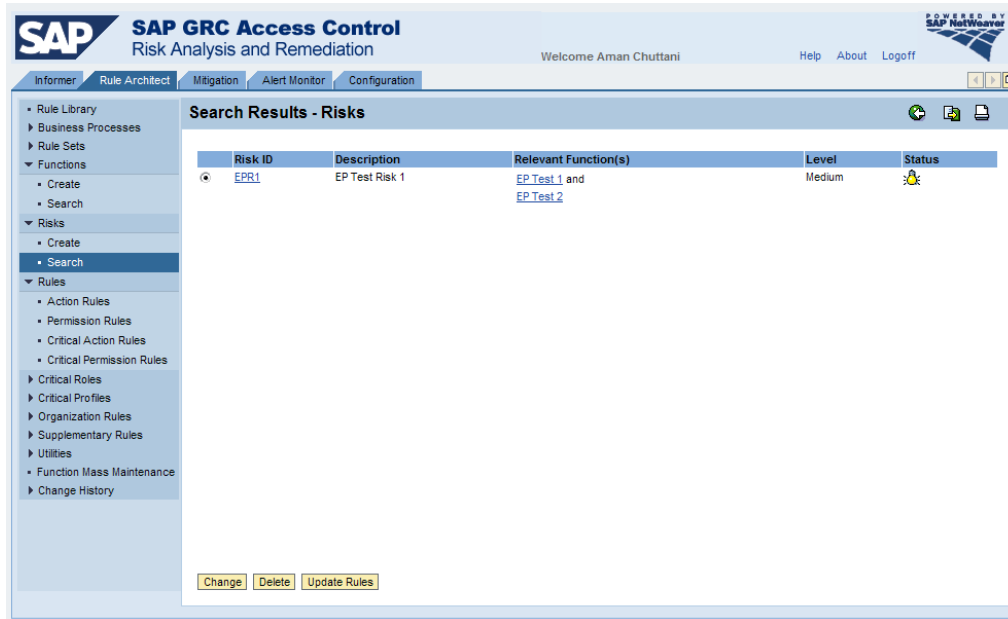
Below the form, there are five tabs: 'Conflicting Functions', 'Detailed Description', 'Control Objective', 'Risk Owners', and 'Rule Sets'. The 'Conflicting Functions' tab is selected, showing a list of functions with a search bar and a 'Save' button. The function list includes:

- Function \*
- EP Test 1 (EP01)
- EP Test 1 (EP01)
- EP Test 2 (EP02)
- FA01 - Maintain Asset Document (FA01)
- FA02 - Maintain Asset Master (FA02)
- FI01 - Revenue Reposting (FI01)
- FI02 - Activity Allocation (FI02)
- FI03 - Bank Reconciliation (FI03)
- FI04 - Maintain Bank Master Data (FI04)
- FI05 - Product Costing (FI05)
- FI06 - Maintain Posting Periods (FI06)

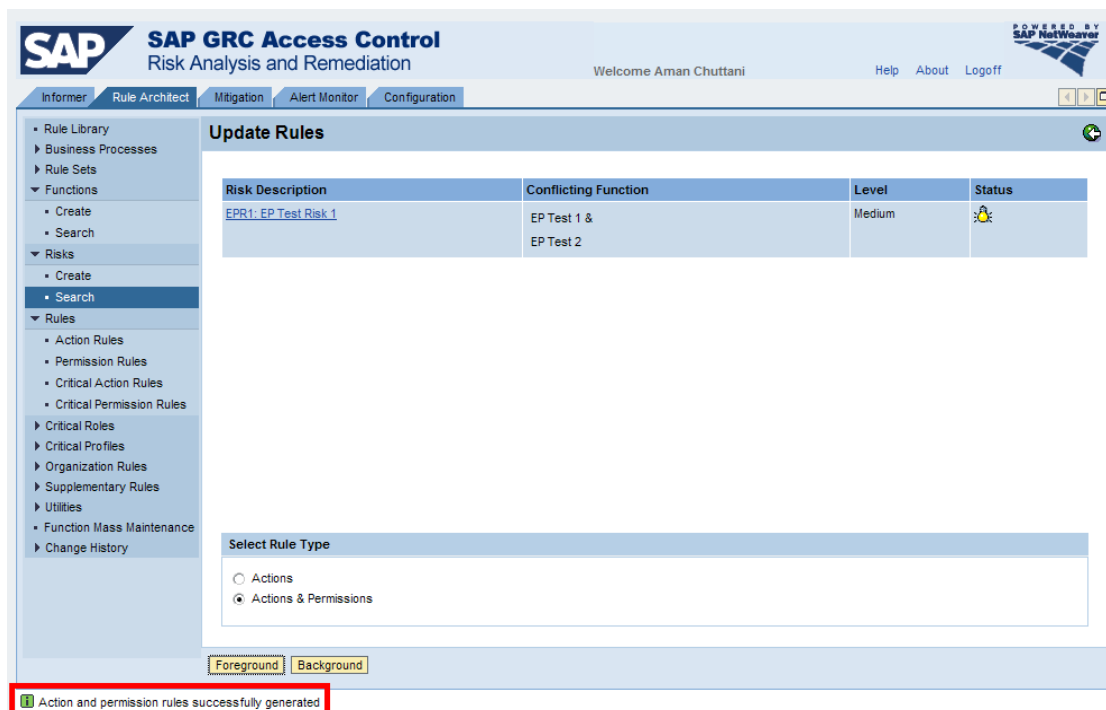
7. Click Save.

## Generate Rules Individually

1. Log-in to the RAR application with following link as business process owner.  
<http://<server-id>:<port-id>/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCalibrator>
2. Go to Rule Architect Tab.
3. Go to Risks -> Search. Search for the particular risk defined for the EP System.



4. Click Update Rules.
5. Select Action and Permission Rules and click Foreground.
6. Once the process completes successfully message would be displayed at the bottom of the web-page.



## Mass Generation of Rules

1. Log-in to the RAR application with following link as business process owner.

<http://<server-id>:<port-id>/webdynpro/dispatcher/sap.com/grc~ccappcomp/ComplianceCalibrator>

2. Go to Rule Architect Tab
3. Go to Rule Upload -> Generate Rules.
4. Click Foreground or Background to generate Rules.

The screenshot displays the 'Generate Rules' screen in the SAP GRC Access Control application. The left sidebar contains a navigation menu with categories like Risk Analysis, Mitigating Controls, and Rule Upload. The main area shows a table of generated rules:

Rule ID	Description	Associated Objects	Risk Level	Enablement
D019	Commission / Incentives may be paid based on the number of sales orders	CR04 - Process CRM Sales Order & PY04 - Process Payroll	High	Enable
D020	Add items to product catalogs and create fictitious sales orders for those items	CR04 - Process CRM Sales Order & CR10 - Maintain Product Catalog	Medium	Enable
EPR1	EP Test Risk 1	EP Test 1 & EP Test 2	Medium	Enable
F001	Maintain fictitious GL account & hide activity via postings	GL01 - Post Journal Entry & GL02 - Maintain GL Master Data	Medium	Enable
F002	Alter a cost center and process unauthorized cost transfers	CC03 - Maintain Cost Centers & CC06 - Cost Transfer Processing	Medium	Enable
F003	Alter a cc and process unauthorized revenue entries	CC03 - Maintain Cost Centers & FI01 - Revenue Reposting	Medium	Enable
F004	Manipulate cc reports to hide inappropriate journal entries	CC02 - Maintain CC or CE Groups & GL01 - Post Journal Entry	Medium	Enable
F005	Maintain bank account and post a payment from it	AP01 - AP Payments & FI04 - Maintain Bank Master Data	High	Enable
F006	Pay a vendor invoice and hide it via asset depreciation	AP02 - Process Vendor Invoices &	High	Enable

At the bottom of the table, there are two buttons: 'Foreground' and 'Background'.

5. Action and Permission Rules would be generated for all the risks.

## Related Content

You can also refer to the following documents on SAP BPX Community.

- [SAP GRC How-to Guides](#)
- [SAP GRC Access Control Application Integration](#)
- [SAP GRC Integrate GRC AC53 CUP and NW IdM](#)

For more information, visit the [Governance, Risk, and Compliance homepage](#).

## Copyright

© 2008 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, System i, System i5, System p, System p5, System x, System z, System z9, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, Informix, i5/OS, POWER, POWER5, POWER5+, OpenPower and PowerPC are trademarks or registered trademarks of IBM Corporation.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

These materials are provided "as is" without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall not be liable for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials.

SAP does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third party web pages nor provide any warranty whatsoever relating to third party web pages.

Any software coding and/or code lines/strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.