Purpose of this document

This document allows implementation consultants and administrators to setup the required functionality for creating a single role in AC after the post-installation has been finished. This is by no means a comprehensive guide for setting up the Business Role Management component, rather it allows testing the application is working properly by setting up a basic test case.
Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided 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 assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.
Agenda

- **Requirements**
  - Assigning connectors to the connector groups
  - Adding connector to required scenario
  - Associating actions and assign default connectors
  - Activating BC Sets
  - Verifying configuration parameters
  - Assigning roles and maintaining AC owners

- **Configuration**
  - Maintain Role Type Settings
  - Customizing Role Attributes
  - Customizing the Methodology Process (optional)
  - Creating Role Approval Workflow

- **Creating a single role**
Requirements

• Assigning connectors to the connector groups
• Adding connector to required scenario
• Associating actions and assign default connectors
• Activating BC Sets
• Verifying configuration parameters
• Assigning roles and maintaining AC owners
Assigning connectors to the connector groups

Define connector groups to be used as landscapes with group type “Logical Group” and link the systems under “Assign Connectors to Connector Groups”
Adding connector to required scenarios

For Role Management it is required to have the ROLMG, AUTH and PROV scenarios linked to the connector, this is done via IMG:

![Image of Governance, Risk and Compliance menu with highlighted options]

![Image of Change View "Scenario-Connector Link": Overview table]

<table>
<thead>
<tr>
<th>Integration Scenario</th>
<th>ROLMG</th>
<th>Role Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub Scenario</td>
<td>ROLMG</td>
<td>Role Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Target Connector</th>
<th>Con.Type</th>
<th>Connection Type Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZMGCLNT800</td>
<td>SAP</td>
<td>SAP System</td>
</tr>
</tbody>
</table>
Associating actions and assigning default connectors

Go to Access Control → Maintain Mapping for Actions and Connector Groups

Maintain again the connector group and make sure the flag Active is set.

Then assign the default connectors for action 1 to 4, make sure there is at least one default per action.
Activating the BC Sets

Rule sets are enabling using BC sets via transaction code **SCPR20**

Make sure the respective BC Sets were enabled as described in the post-installation slides:

- GRAC_ROLE_MGMT_LANDSCAPE
- GRAC_ROLE_MGMT_METHODOLOGY
- GRAC_ROLE_MGMT_PRE_REQ_TYPE
- GRAC_ROLE_MGMT_ROLE_STATUS
- GRAC_ROLE_MGMT_SENTIVITY
Verifying default configuration parameters

Please check the configuration parameters related to role management are properly set according to your needs.

<table>
<thead>
<tr>
<th>New Entries: Overview of Added Entries</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>AC Configuration settings</th>
<th>Param ID</th>
<th>Parameter Value</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Management</td>
<td>3000</td>
<td>Default Business Process</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3001</td>
<td>Default Subprocess</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3002</td>
<td>Default Critical Level</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3003</td>
<td>PROD</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3004</td>
<td>DEV</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3005</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3006</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3007</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3008</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3009</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3010</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3011</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3012</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3013</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3014</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3015</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3016</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3017</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3018</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3019</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3020</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Role Management</td>
<td>3021</td>
<td>/sap-grc/import</td>
<td></td>
</tr>
</tbody>
</table>

© 2011 SAP AG. All rights reserved.
Creating users and assigning roles

The responsible person for role content need to be created with the respective roles in the AC system. Please note these roles are provided as examples and customer roles should be created based on their authorizations.

- **In the AC system**
  - Role: User who is Role Owner
  - Role: SAP_GRAC_ROLE_MGMT_ROLE_OWNER

**Reminder:** end users will require also the roles based on SAP_GRC_FN_BASE and SAP_GRC_FN_BUSINESS_USER
Maintaining AC owners

Go to NWBC → Access Management → Access Control Owners and maintain the owners as shown below:

After this is done it is possible to configure these users as role owners
Configuration

- Maintain Role Type Settings
- Customizing Role Attributes
- Customizing the Methodology Process
- Creating Role Approval Workflow
Maintain Role Type Settings

Go to IMG, Access Control → Maintain Role Type Settings

- Activate role types *(mandatory)*
- Maintain role types *(optional)*
- Define the maximum length for the role types per application type *(optional)*
Customizing Role Attributes

Define Business and Subprocesses in IMG under **mandatory**

Specify Naming Convention **optional**

Define Role Attributes
  - Maintain Project Release **mandatory**
  - Role Sensitivity **optional**
  - Critical Level **optional**
  - Companies **optional**
  - Functional Areas **optional**
  - Prerequisite Types **optional**

Create Organizational Value Mapping **optional**
The customizing steps for “BRF+ Rule Creation” and “Methodology Process Definition” are **not** necessary when the default methodology process is used for all roles.

### Customizing the Methodology Process (optional)

#### Overview

The customizing steps for “BRF+ Rule Creation” and “Methodology Process Definition” are **not** necessary when the default methodology process is used for all roles.
Customizing the Methodology Process (optional)
Create the BRF+ Function

Run the program GRAC_GENERATE_ERM_BRFRULE to create the BRF+ application and function
Customizing the Methodology Process (optional)
Maintain the BRF+ Function

Go to BRF+ and define the decision table for the methodology process
Customizing the Methodology Process (optional)
Define the Methodology Process and Steps

Create the different methodology processes and include the required steps
Customizing the Methodology Process (optional)
Assign the BRF+ Rule to the Methodology Process

Assign the BRF+ Application Name and the BRF+ Function Name to the Condition Group “METHODOLOGY”:

Assign the BRF+ Condition Group ID to the methodology process ID:
Creating Role Approval Workflow
Maintain MSMP Workflow

A default workflow process can be used to set up easy the approval workflow for the role content

Select in step 1 the workflow process SAP_GRAC_ROLE_APPR
Creating Role Approval Workflow

Maintain Approver

Maintain in step 5 the agent ID GRAC_ROLE_APPROVER and the task settings

Save and activate the workflow in step 7
Creating a single role
Creating a single role

Now you should be able to create a single role.

Go to Access Management Workcenter and select Role Maintenance.