

SAP Governance, Risk & Compliance

Access Control 5.3

Post-Installation

- Enterprise Role Management
- Part I: Configuration



Frank Rambo, SAP GRC RIG, EMEA Region



Frank Bannert, SAP GRC RIG, EMEA Region

- We belong to the GRC Regional Implementation Group (RIG) located in USA, Germany and India
- As recognized experts, our mission is to enable others to successfully implement SAP GRC solutions.
- We ensure:
 - high-adoption rates,
 - 100% customer satisfaction, and customer references.
- We are committed to continuous improvement of GRC products and services



- We recommend the following installation methodology
 1. Install SAP Netweaver AS JAVA 7.0 SP12+
 2. Run Pre-Installation Presentation
 3. Deploy Access Control Software (including latest Support Packages)
 4. Run Post-Installation Presentations (also available as Flash Movie)
 - a. Post-Installation Risk Analysis and Remediation
 - b. Post-Installation Superuser Privilege Management
 - c. Post-Installation Compliant User Provisioning
 - d. Post-Installation Enterprise Role Management
 - **Part I: Configuration**
 - Part II: Testing SAP GRC Default Process
 5. Start Customizing Access Control 5.3 according to customer requirements

Post-Installation Activities - Enterprise Role Management -



1. Upload UME Roles (→ Refer to Post-Installation Slide Deck for RAR)
2. Initial System Data Import into ERM
3. Configuration of Miscellaneous Settings in ERM
4. Configuration for Compliant User Provisioning
5. System Landscape Definition
6. Run Initial Synchronization Background Jobs
7. Definition of Role Attributes
8. Role Methodology & Condition Groups
9. Definition of Approval Criteria
10. Definition of Naming Conventions
11. Definition of Organizational Value Mapping

2 – Import of Initial System Data → Upload Initial Data into ERM



Upload the following xml files with Initial System Data:

- *RE_init_clean_and_insert_data.xml* - select the **Clean and Insert** option.
- *RE_init_append_data.xml* - select the **Append** option.
- *RE_init_methodology_data.xml* - select the **Append** option.

The screenshot shows the SAP GRC Access Control Enterprise Role Management interface. The left sidebar contains a navigation tree with 'Initial System Data' selected. The main area displays the 'Import Data' dialog. The 'File Name' field contains 'S:\3\JAVAW\IRRE\RE_init_clean_insert_data.xml' and has a 'Browse...' button. Below the file name, there are three radio button options: 'Insert', 'Append', and 'Clean and Insert'. The 'Clean and Insert' option is selected. An 'Import' button is located below the radio buttons. The dialog is highlighted with an orange border.

This fills data into:
Config. → Role Status
Config. → Methodology
Config. → Configuration Settings

3 – Configuration for RAR & Miscellaneous (1/5)



Check Next Slide!

Role Management | Informer | Configuration

- Role Attributes
 - Business Process
 - Sub-Process
 - Functional Area
 - Custom Fields
 - Project/Release
- Role Status
- Naming Convention
- Org. Value Mapping
- Condition Groups
 - Methodology
 - System Landscape
 - Workflow
 - Log History
- Background Jobs
- Miscellaneous
 - Transaction Import
 - Mass Role Import
 - Role Usage Synchronization
 - Initial System Data
 - Configuration Settings
 - Administration
 - Migration from 4.0
 - Upgrade

Allow role generation with violations [No]

This option enables you to configure whether the role can be generated despite violations. If you set this configuration to "No", then you will not be able to generate the role unless all the role violations are taken care of

Allow Role Generation on Multiple Systems [Yes]

This option enables you to configure whether role can be generated on multiple systems

Use logged on user credentials for role generation [No]

This option enables you to configure whether the logged-on user credentials should be used during role generation. If this option is set to "No", then the target back-end system user ID and password is used

Analysis Type [Object]

This option enables you to specify a default analysis level. If you set this configuration value to "Object", then the risk analysis by default will be performed at the object level; otherwise, it will be performed at the "TCode" level

Web Service Info. for CC Risk Analysis

This option allows you to set Web Service URL for risk analysis

Do not use Web Service; CC deployed on the same server
 Use Web Service

Web Service Info. for CC Transaction Usage

This option allows you to set Web Service URL for transaction usage.

Web Service URL:

User Name:

Password:

Web Service Info. for CC Mitigation Control

This option allows you to set Web Service URL for Mitigation Control. Make sure that mitigation web service and risk analysis service exist on the same server

Web Service URL:

User Name:

Password:

- Configuration → Miscellaneous (Check SAP Note 1175227):
 - Allow Role Generation with Violations: **No** (customer selection)
 - Allow Role Generation with Multiple Systems: **Yes**
 - Use Logged-in user credentials for Role Generation: **No** (→ Backend RFC User Logon)
 - Analysis Type: Object (Risk Analysis on object or only transaction level)
 - Web Service Info for CC Risk Analysis
 - EJB Call: Select **Do not use Web Service; Risk Analysis and Remediation deployed on the same server.**
 - Web Service Info for Risk Analysis and Remediation Transaction Usage
 - URL: `http://<server>:<port>/VirsaCCActionUsageService/Config1?wsdl&style=document`
 - User Name: <User ID> (with UME Role *VIRSA_CC_ADMINISTRATOR*)
 - Password: <password>
 - Web Service Info for CC Mitigation Control
 - URL: `http://<server>:<port>/VirsaCCMitigation5_0Service/Config1?wsdl&style=document`
 - User Name: <User ID> (with UME Role *VIRSA_CC_ADMINISTRATOR*)
 - Password: <password>

3 – Configuration for RAR & Miscellaneous (3/5)



Check Next Slide!

| | |
|--|--|
| <ul style="list-style-type: none">▼ Role Attributes<ul style="list-style-type: none">▪ Business Process▪ Sub-Process▪ Functional Area▪ Custom Fields▪ Project/Release▪ Role Status▪ Naming Convention▪ Org. Value Mapping▪ Condition Groups<ul style="list-style-type: none">▶ Methodology▶ System Landscape▶ Workflow▶ Log History▪ Background Jobs▪ Miscellaneous▪ Transaction Import▪ Mass Role Import▪ Role Usage Synchronization▪ Initial System Data▪ Configuration Settings<ul style="list-style-type: none">▶ Administration▶ Migration from 4.0▪ Upgrade | <p>Web Service Info. for CC Functions</p> <p>This option allows you to set Web Service URL for Functions</p> <p>Web Service URL <input type="text" value="http://iwdtvm2450:50000/irsaCCF"/></p> <p>User Name <input type="text" value="ac_admin"/></p> <p>Password <input type="password" value="*****"/></p> |
| | <p>Web Service Info. for AE Workflow</p> <p>This option allows you to set Workflow URL for role approval</p> <p>Workflow URL <input type="text" value="http://iwdtvm2450:50000/AEWFR"/></p> |
| | <p>Allow editing org. level values for derived roles</p> <p>This option enables you to edit org. level values for derived roles. If the value is set to "No", you cannot edit org. Level values for derived roles</p> <p><input type="text" value="Yes"/></p> |
| | <p>Allows you to add a function to an authorization</p> <p>This option allows you to add functions to authorizations</p> <p><input type="text" value="Yes"/></p> |
| | <p>Add objects to a role</p> <p>This option enables you to add objects to a role directly. If the value is set to "Yes", then you can add objects directly to the role authorization data, or else you can add objects to a role only by adding functions and/or transactions</p> <p><input type="text" value="Yes"/></p> |
| | <p>Ticket number after authorization data changes</p> <p>This option allows you to specify whether you need to enter a ticket number after making additions or changes to the authorization data in a role. If the value for this option is set to "Yes", then after you save any additions or changes you make to the authorization data in a role, you will be prompted for a ticket number. If the value for this option is set to "No", then you will not be prompted for a ticket number</p> <p><input type="text" value="Yes"/></p> |



- Configuration → Miscellaneous:
 - Web Service Info for CC Functions
 - URL: `http://<server>:<port>/VirsaCCFunction5_0Service/Config1?wsdl&style=document`
 - User Name: `<User ID>` (with UME Role `VIRSA_CC_ADMINISTRATOR`)
 - Password: `<password>`
 - Web Service Info for AE Workflow
 - URL:
`http://<server>:<port>/AEWFRequestSubmissionService_5_2/Config1?wsdl&style=document`
 - Allow Editing Org. Level values for derived roles: **Yes** (customer selection)
 - Allows you to add function to an authorization: **Yes**
 - Add objects to a role: **Yes**
 - Ticket number after authorization data changes: **Yes** (customer selection)

3 – Configuration for RAR & Miscellaneous (5/5)



- Configuration → Miscellaneous:
 - Allow Editing Role Authorizations in PFCG: **Yes**
 - Upload Directory: **<path on AC server for file uploads from ERM>** (only temporarily needed when upgrading from RE5.2. In ERM 5.3 all attachments are saved in the database)
 - Log Level: **Error** (customer selection)
 - Default Language: **English** (customer selection)
 - Number of concurrent background jobs: **3**
 - Allows you to attach files to a role definition
 - This option allows you to attach files to a role: **Yes**
 - This option allows you to set the file size (in KB): **1000**

The screenshot shows the SAP configuration interface for the 'Miscellaneous' category. On the left is a navigation menu with options like 'Background Jobs', 'Miscellaneous', 'Transaction Import', 'Mass Role Import', 'Role Usage Synchronization', 'Initial System Data', 'Configuration Settings', 'Administration', 'Migration from 4.0', and 'Upgrade'. The main area contains several configuration sections:

- Allow Editing Role Authorizations in PFCG**: A dropdown menu set to 'Yes'. Description: 'This option enables you to configure whether the role can be opened and edited in PFCG. If you set this configuration to "No", you cannot create or edit the role in PFCG.'
- Upload Directory**: A text input field containing 'tmp'. Description: 'This option allows you to set a default folder for all the files uploaded from Enterprise Role Management'
- Log Level**: A dropdown menu set to 'Error'. Description: 'This option enables you to configure the log level'
- Default Language**: A dropdown menu set to 'English'. Description: 'This option enables you to set the default language.'
- Number of concurrent background jobs**: A text input field containing '3'. Description: 'This option allows you to limit the number of background jobs that can be run concurrently.'
- Allows you to attach files to role definition**: A dropdown menu set to 'Yes'. Description: 'This option allows you to attach files to a role'. Below this is another text input field containing '1000'. Description: 'This option allows you to set the file size (in KB)'

A 'Save' button is located at the bottom left of the configuration area.

4 – Configuration for CUP (1/8)

→ Upload Initial Data into CUP



- To enable workflows for role approval the file *AE_init_append_data_RE.xml* - with **Append** option - must be uploaded in **CUP** → Configuration → Initial System Data

The screenshot shows the SAP GRC Access Control interface. The main title is 'SAP GRC Access Control Compliant User Provisioning'. The navigation bar includes 'My Work', 'Informer', and 'Configuration'. The left sidebar shows a tree view of configuration options, with 'Initial System Data' selected. The main content area displays the 'Initialize DB' dialog box. The 'Import Data' section is highlighted with an orange border and contains the following information:

File Name: S:\JAVAV\WIRRE\AE_init_append_data_RE.xml | Browse...
 Insert
 Append
 Clean and Insert

Below the 'Import Data' section is an 'Export Data' table with the following columns: Name, Description.

| <input type="checkbox"/> | Name | Description |
|--------------------------|------------------------|------------------------|
| <input type="checkbox"/> | Initial Data | Initial Data |
| <input type="checkbox"/> | Connector | Connector |
| <input type="checkbox"/> | Roles | Roles |
| <input type="checkbox"/> | Workflow Configuration | Workflow Configuration |
| <input type="checkbox"/> | User Defaults | User Defaults |
| <input type="checkbox"/> | Hr Triggers | Hr Triggers |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |

Buttons for 'Import' and 'Export' are visible at the bottom of the dialog box.

4 – Configuration for CUP (2/8)

→ Check Request Type for ERM



- In CUP → Configuration → Request Configuration → Request Type
- Check that Request Type *RE_ROLE_APPROVAL* exists
- Make sure it has workflow *RE*

The screenshot shows the SAP GRC Access Control interface. The main content area displays a table titled "Request Configuration" with the following data:

| Request Type | Description | Category | Priority | Access Enforcer | Workflow |
|--|-----------------------------|---|----------|--------------------|----------|
| <input type="checkbox"/> RISKU | Update Risk | Update Risk | 0 | Access Enforcer | |
| <input type="checkbox"/> CHANGE | Change Account | Changes to an Existing Account | 1 | Access Enforcer | |
| <input type="checkbox"/> DELETE | Delete Account | Account Deletions | 2 | Access Enforcer | |
| <input type="checkbox"/> INFORMATION | Information | Information | 3 | Access Enforcer | |
| <input type="checkbox"/> LOCK | Lock Account | Locking Accounts | 4 | Access Enforcer | |
| <input type="checkbox"/> NEW | New Account | New Account | 5 | Access Enforcer | |
| <input type="checkbox"/> UNLOCK | Unlock Account | Unlocking Accounts | 6 | Access Enforcer | |
| <input type="checkbox"/> SUPER_USER_ACCESS | Superuser Access | Superuser Access | 7 | Access Enforcer | |
| <input type="checkbox"/> NEW ERP ACCOUNT | New ERP account | New ERP account | 8 | Access Enforcer | |
| <input type="checkbox"/> NEW_SAP | New Account for Company SAP | New Account for Company SAP | 9 | Access Enforcer | |
| <input type="checkbox"/> TEST HR TERMINATION | Test HR Termination | Test HR Termination | 10 | Access Enforcer | |
| <input type="checkbox"/> ROLE_APPROVAL | ERM Role Approval | ERM Role Approval | 0 | RE | |
| <input type="checkbox"/> RE_ROLE_APPROVAL | RE Role Approval | Request Type for Role Expert Role Content Approval | 2 | RE | |
| <input type="checkbox"/> ROLE_REAFFIRM | Role Reaffirm | Role Reaffirm | 0 | Role Reaffirm | |
| <input type="checkbox"/> SOD_REVIEW | SOD Review | SOD Review | 8 | SOD Review | |
| <input type="checkbox"/> UAR_REVIEW | User Access Review | User Access Review | 0 | User Access Review | |

Buttons: Create, Change, Delete

4 – Configuration for CUP (3/8)

→ Check, if Priority for ERM exists



- Check, if a priority *RE_HIGH* for workflow type „RE“ exists
- If not, create it accordingly.

The screenshot shows the SAP GRC Access Control interface. The main window displays the 'Request Configuration' table with the following data:

| Priority | Short Description | Description | Workflow Type |
|---|-------------------|-------------|--------------------|
| <input type="checkbox"/> AE_HIGH | AE_HIGH | AE_HIGH | Access Enforcer |
| <input type="checkbox"/> AE_LOW | AE_LOW | AE_LOW | Access Enforcer |
| <input type="checkbox"/> DEFAULT | default | default | Access Enforcer |
| <input checked="" type="checkbox"/> RE_HIGH | RE High | RE High | RE |
| <input type="checkbox"/> SOD_HIGH | SOD High | SOD High | SOD Review |
| <input type="checkbox"/> UAR_HIGH | UAR High | UAR High | User Access Review |

A 'Modify Priority' dialog box is open, showing the following fields:

- Priority*: RE_HIGH
- Workflow Type: RE
- Short Description*: RE High
- Description*: RE High

Buttons: Create, Change, Delete, Save, Cancel

4 – Configuration for CUP (4/8)

→ Create a workflow initiator for ERM



- Go to CUP → Configuration → Workflow → Initiator and create an initiator
 - Workflow type: RE
 - Attributes: Request Type = RE Role Approval & Priority = RE_HIGH

Initiator

Name*

Short Description*

Description

Workflow Type*

Select Attributes

Condition

Attribute *

Value*

Select Attributes [Filter](#)

| <input type="checkbox"/> | Condition | Attribute | Value |
|--------------------------|-----------|--------------|------------------|
| <input type="checkbox"/> | AND | Priority | RE High |
| <input type="checkbox"/> | AND | Request Type | RE Role Approval |
| <input type="checkbox"/> | | | |
| <input type="checkbox"/> | | | |
| <input type="checkbox"/> | | | |
| <input type="checkbox"/> | | | |
| <input type="checkbox"/> | | | |
| <input type="checkbox"/> | | | |
| <input type="checkbox"/> | | | |
| <input type="checkbox"/> | | | |
| <input type="checkbox"/> | | | |

4 – Configuration for CUP (5/8) → Create a CAD for ERM



- Go to CUP → Configuration → Workflow → Custom Approver Determinator
 - CAD Type: Web Service
 - Workflow Type: RE
 - URI: `http://<server>:<port>/AEWFCADApproversServiceWS_5_2/Config1?wsdl&style=document`
 - User Name / Password: User with AC Administrator UME-Roles

The screenshot shows the SAP GRC Access Control interface. The main title is "SAP GRC Access Control Compliant User Provisioning". The navigation bar includes "My Work", "Informer", and "Configuration". The left sidebar shows a tree view with "Workflow" expanded to "Custom Approver Determinators". The main content area is titled "Create Approver Determinator" and contains the following fields:

| Approver Determinator | |
|-----------------------|-------------------|
| Name: | ERM_ROLE_APPROVER |
| Short Description*: | ERM Role Approval |
| Description: | ERM Role Approval |
| CAD Type*: | Web Service |
| Workflow Type*: | RE |

| Web Service Details | |
|---------------------|---|
| URI*: | ServiceWS_5_2/Config1?wsdl&style=document |
| User Name: | ac_admin |
| Password: | |

Buttons: Save, Cancel

4 – Configuration for CUP (6/8)

→ Create a Stage for ERM Role Approval WF



- Create at least one stage for ERM approval workflow
- Go to CUP → Configuration → Workflow → Stage and create a stage
 - Workflow Type: RE
 - Approver Determinator: ERM_ROLE_APPROVER (created just before)

The screenshot shows the SAP GRC Access Control interface for configuring a stage. The main window is titled "Stage Configuration" and is divided into two sections: "Stage Details" and "Notification Configuration".

Stage Details:

| | |
|---------------------------|-------------------|
| Name* | ERM_ROLE_APPROV |
| Short Description* | ERM Role Approver |
| Description | ERM Role Approver |
| Workflow Type* | RE |
| Approver Determinator* | ERM_ROLE_APPROVER |
| Request Wait Time (Days) | 0 |
| Request Wait Time (Hours) | 0 |
| Escalation Configuration | No Escalation |

Notification Configuration:

| | | |
|------------------|------------------------------------|--|
| Approved | <input type="checkbox"/> Requestor | <input type="checkbox"/> Other Approvers |
| Escalated | <input type="checkbox"/> Requestor | <input type="checkbox"/> Other Approvers |
| Request Rejected | <input type="checkbox"/> Requestor | <input type="checkbox"/> Other Approvers |

Below the notification configuration, there are tabs for "Approved", "Request Rejected", "Escalation", and "Next Approver". The "Request Rejected" tab is currently selected. The "Content" field is visible, showing a rich text editor with options for style, font, size, and email arguments.

4 – Configuration for CUP (7/8)

→ Create a Path for ERM Role Approval WF



- Create a path for ERM approval workflow
- Go to CUP → Configuration → Workflow → Path and create a path
 - Workflow Type: RE
 - Number of Stages: 1 (but more possible)
 - Initiator: ROLE_APPROVAL (created just before)
 - Active: Checked
 - Stage 1: ERM_ROLE_APPROVER

The screenshot shows the SAP CUP Path Definition interface. On the left is a navigation tree with 'Path' selected. The main area is titled 'Create Path' and contains a table with the following data:

| Name* | Short Description* | Description | Workflow Type* | Number of Stages* | Initiator* | Active | Detour |
|-------------------|--------------------|-------------------|----------------|-------------------|---------------|-------------------------------------|--------------------------|
| ERM_ROLE_APPROVAL | ERM Role Approval | ERM Role Approval | RE | 1 | ROLE_APPROVAL | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Below the table is the 'Path Definition For Path:' section, which shows a flow diagram:

- Start (oval)
- ↓
- Stage 1: ERM_ROLE_APPROVAL (dropdown menu) with Approver Determinator: ERM_ROLE_APPROVER
- ↓
- Finish (oval)

At the bottom are buttons: Create, Change, Delete, Save, Cancel.

4 – Configuration for CUP (8/8)

→ Configure Exit Web Service



- Go to CUP → Configuration → Miscellaneous
 - Exit URI: http://<server>:<port>/AEWFExitServiceWS_5_2/Config1?wsdl&style=document
 - User Name: User with AC Administrator UME-Roles
 - Password: <password>
 - Active: Checked

| Workflow Types | | | | | | |
|----------------|-------------------------------------|--------------------|-------------------------------------|-----------|----------|-------------------------------------|
| Name | Description | Short Description | Exit URI | User Name | Password | Active |
| AE | Access Enforcer | Access Enforcer | | | | <input checked="" type="checkbox"/> |
| MITICTRL | This is a workflow type for creatin | Mitigation Control | http://wdfvm2450.wdf.sap.corp:5i | ac_admin | | <input checked="" type="checkbox"/> |
| MITIOBJ | This is a workflow type for creatin | Mitigation Object | http://wdfvm2450.wdf.sap.corp:5i | ac_admin | | <input checked="" type="checkbox"/> |
| RE | Role Expert | RE | http://wdfvm2450.wdf.sap.corp:50000 | ac_admin | | <input checked="" type="checkbox"/> |
| RISK | This is a workflow type for creatin | Risk | http://wdfvm2450.wdf.sap.corp:5i | ac_admin | | <input checked="" type="checkbox"/> |
| ROLE_RFM | Role Reaffirm | Role Reaffirm | | | | <input checked="" type="checkbox"/> |
| SOD_REVIEW | SOD Review | SOD Review | http://wdfvm2450.wdf.sap.corp:5i | ac_admin | | <input checked="" type="checkbox"/> |
| UAR_REVIEW | User Access Review | User Access Review | http://wdfvm2450.wdf.sap.corp:5i | ac_admin | | <input checked="" type="checkbox"/> |

Save

5 – System Landscape Definition (1/4)

→ Create Systems with SLD Integration



- Create for each backend system a System in ERM → Configuration → System Landscape → Systems.
- Make sure you have already created JCo destination in Netweaver stack with correct naming as explained in *Post-Installation Slide Deck – SPM* page 17-21.
- Select System Type SAP and check SLD Connector checkbox and click on magnifying glass to select JCo from SLD.

The screenshot shows the 'Create System' form in SAP GRC Access Control. The 'System Type' is set to 'SAP'. The 'SLD Connector' checkbox is checked. A magnifying glass icon is highlighted, which opens the 'SLD Connector Search' dialog box. This dialog box displays a table of available systems for selection.

| System | Client | Active |
|-----------------------|--------|--------|
| AR1 | 001 | true |
| VIRSAXSR3_01_MODEL | 001 | true |
| VIRSAXSR3_01_METADATA | 001 | true |

5 - System Landscape Definition (2/4)

→ Test Connection and Fill-In Dummy Values



- Maintain manually the following fields: *Application Server Host*, *System Number* – otherwise the profile generator won't be started correctly – and *SAP Version*.
- Now, maintain the remaining empty mandatory fields *Password*, *Message Server* name with arbitrary dummy values. They are directly read from SLD.
- Click on “Test Connection” and save.

The image displays two screenshots of SAP system configuration forms, illustrating the process of testing a connection and saving the configuration.

Left Screenshot: Create System

- System Type: SAP
- SLD Connector:
- Name*: AR1
- Description:
- Application*: AR1
- Application Server Host*:
- System Number*:
- Client*: 001
- User ID*: webuser
- Password*:
- System Language: EN
- Message Server Name*:
- Message Server Group: SPACE
- Message Server Host: grc-rig-03
- SAP Version*: -Select-

Right Screenshot: Change System

- System Type: SAP
- SLD Connector:
- Name*: AR1
- Description: AR1
- Application*: AR1
- Application Server Host*: grc-rig-03.pal.sap.corp
- System Number*: 00
- Client*: 001
- User ID*: webuser
- Password*:
- System Language: EN
- Message Server Name*: dum
- Message Server Group: SPACE
- Message Server Host: grc-rig-03
- SAP Version*: MySAP ERP 2005

Arrows indicate the flow of data from the 'Create System' form to the 'Change System' form. A 'Connection successful' message is displayed at the top left of the 'Create System' form, indicating the result of the 'Test Connection' action.

5 – System Landscape Definition (3/4)

→ Create System Landscape



- First create a System Landscape for each backend system landscape you want to create/maintain/generate roles for.
- Then assign systems to it – normally the DEV and PRD backend – here in the example we only have a DEV called AR1. Then Associate Actions (next slide)

The screenshot displays two SAP windows. The top window, 'Create Landscape', has the following fields: Name* (ERP), Description* (ERP SAP Landscape), Status* (Enabled), and Type* (SAP). It includes 'Save' and 'Assign Systems' buttons. The bottom window, 'Assign Systems to Landscape', shows 'Landscape: ERP' and a table with the following data:

| System | Description | Status | Associated Actions |
|------------------------------|-------------|--------|--------------------|
| <input type="checkbox"/> AR1 | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

At the bottom of the 'Assign Systems to Landscape' window, there are 'Save', 'Cancel', and 'Associate Actions' buttons. An orange arrow points from the 'Associate Actions' button to a yellow box containing the text 'Check Next Slide!'.

5 – System Landscape Definition (4/4) → Assign Systems to Actions



- Per backend system landscape you have to assign to two different Actions:
 - **Role Risk Analysis** → Assigned to PRD, because risks are defined with respect to the productive systems. In the example below we had only one system available.
 - **Role Generation** → Assigned DEV, because roles still need to undergo their usual testing, which starts in DEV (unit tests), then continues in QA (integration test) etc.

Associate Actions

| Landscape: ERP

Role Risk Analysis

| <input type="checkbox"/> Connector | Type | Default |
|------------------------------------|------|---------|
| <input type="checkbox"/> AR1 | | |
| | | |
| | | |
| | | |

Role Generation

| <input type="checkbox"/> Connector | Type | Default |
|------------------------------------|------|---------|
| <input type="checkbox"/> AR1 | | |
| | | |
| | | |
| | | |

6 – Run Initial Synchronization Background Jobs



- There are three types of (static) background jobs:
 - **Org Value Sync:** Synchronizes the organizational values in Enterprise Role Management with the SAP ERP backend system → Takes 2 min.
 - **Transaction/Object/Field Sync:** Synchronizes the Transaction, Object, and Field values with the SAP backend system → Takes on slow hardware up to 5 hours!
 - **Activity Sync:** Synchronizes Activity field values → Takes 5 min.
- We recommend running these jobs in sequential order. So, wait until a job has completed before you start the next one.

The screenshot shows the SAP Search Results interface for background jobs. The left sidebar contains a navigation menu with 'Background Jobs' selected. The main area displays a table with columns: Job ID, Task Name, Job Name, Job Type, Start Date, Next Invoke, Recurrence Interval (Sec), User, Status, and Active. Three jobs are listed, all with a status of 'Completed'. Below the table are navigation controls including 'Page 1 / 1' and buttons for 'Create', 'Edit', 'Delete', 'Activate/Deactivate', 'Job History', and 'Refresh'.

| Job ID | Task Name | Job Name | Job Type | Start Date | Next Invoke | Recurrence Interval (Sec) | User | Status | Active |
|--------|-------------------------------|---------------------------------------|-----------|-------------------------|-------------------------|---------------------------|----------|-----------|--------|
| 3 | Activity Value Sync | Initial Activity Value Sync | Immediate | 5/22/08 8:09:25 PM CEST | 5/22/08 8:10:00 PM CEST | 0 | ac_admin | Completed | |
| 2 | Transaction/Object/Field Sync | Initial Transaction/Object/Field Sync | Immediate | 5/22/08 3:46:43 PM CEST | 5/22/08 3:47:00 PM CEST | 0 | ac_admin | Completed | |
| 1 | Org. Value Sync | Initial Org Value Sync | Immediate | 5/22/08 3:41:39 PM CEST | 5/22/08 3:42:00 PM CEST | 0 | ac_admin | Completed | |

7 – Definition of Role Attributes (1/3)

→ Business Processes & Sub-Processes



- Go to ERM → Configuration → Role Attributes → Business Processes and create business processes you want to use as role attributes

The screenshot shows the SAP Role Management Configuration interface. The left sidebar is expanded to 'Role Attributes' > 'Business Process'. The main area is titled 'Create Business Process' and contains the following fields:

| | |
|----------------------|----------------|
| Business Process ID* | PR |
| Description* | Procure to Pay |
| Abbreviation* | PR |

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

- Then create Sub-Processes you want to use as role attributes

The screenshot shows the SAP Role Management Configuration interface. The left sidebar is expanded to 'Role Attributes' > 'Sub-Process'. The main area is titled 'Create Sub-Process' and contains the following fields:

| | |
|-----------------|---------------------------|
| Sub-Process ID* | PR01 |
| Description* | Vendor Master Maintenance |
| Abbreviation* | VM |

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

Definition of Role Attributes (2/3)

→ Map Sub-Processes to Business Processes



- Return to ERM → Configuration → Role Attributes → Business Processes and click on Process Mapping to map Sub-Processes to Business Processes

Associate Business Sub-Process to Business Process

Business process/sub-process association saved successfully

Business Process: Procure to Pay

Search Results

| <input type="checkbox"/> | Sub-Process ID | Description |
|--------------------------|----------------|-----------------------------|
| <input type="checkbox"/> | PR01 | Vendor Master Maintenance |
| <input type="checkbox"/> | PR02 | Production Order Processing |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |

Save Continue

Page 1 / 1

Create Change Delete **Process Mapping** Import Export

7 - Definition of Role Attributes (3/3)

→ Functional Areas, Custom Fields & More



- Go to ERM → Configuration → Role Attributes → Functional Areas and create Functional Areas you want to use as role attributes

The screenshot shows the SAP Role Management Configuration interface. The left sidebar is titled 'Role Attributes' and includes a tree view with 'Functional Area' selected. The main content area is titled 'Create Functional Area' and contains three input fields: 'Functional Area ID*' with the value 'FI', 'Description*' with the value 'Financial', and 'Abbreviation*' with the value 'FI'. A 'Save' button is located at the bottom left of the form.

- Optionally you can create custom fields to have additional role attributes available
- Also, you can create project or release attributes for you roles

The screenshot shows the SAP Role Management Configuration interface. The left sidebar is titled 'Role Attributes' and includes a tree view with 'Project/Release' selected. The main content area is titled 'Create Project/Release' and contains two input fields: 'Project/Release ID*' with the value 'GT10' and 'Description*' with the value 'Global Template Version 1.0'. A 'Save' button is located at the bottom left of the form.

8 – Role Methodology & Condition Groups



- There is already a pre-defined **Methodology Process** available in ERM.

| Process | | | |
|--|-----------------------------------|--------|---------|
| Process | Description | Status | Default |
| <input type="checkbox"/> VIRSA.DEFAULT.PROCESS | Default process provided by Virsa | | |

- We recommend using this process for first tests.
- Then you can create one or **Multiple Methodology** processes according to your business requirements.
- If you create multiple **Methodology Processes**, then you need to create **Condition Groups** and assign one or multiple **Condition Groups** to each **Methodology Process**. However, you cannot assign the same Condition Group to multiple **Methodology Processes**.
- A **Condition Group** is a set of role attributes. Once the role attributes are defined for a new role and match a **Condition Group** the system will apply the corresponding **Methodology Process** for further creation steps of this role.

9 – Definition of Approval Criteria (1/3)



- Approval Criteria are stored as Groups and are used to determine role approver based on the role attributes.
- In the example we determine role approver based on the role attribute Business Process and map to our BP *Procure to Pay (PR)* the responsible approvers. However, you could any combination of role attributes to determine role approvers from.

The screenshot shows the SAP Role Management Configuration interface. The left sidebar contains a tree view with categories: Role Attributes (Business Process, Sub-Process, Functional Area, Custom Fields, Project/Release), Role Status, Naming Convention, Org. Value Mapping, Condition Groups, Methodology (Actions, Step, Process), System Landscape, Workflow, and Approval Criteria. The main area is titled 'Create Approval Criteria' and features a 'Group Name*' field containing 'Role Approver for Business Process PR'. Below this is a table with columns for 'Attribute' and a dropdown menu currently showing 'Business Process'. At the bottom left, there is an 'Assign Approvers' button, which is highlighted with an orange box and an arrow pointing to a yellow callout box containing the text 'Check Next Slide!'.

9 – Definition of Approval Criteria (2/3)



➤ Assign approvers to each business process

Approval Criteria Values
✓ Action successful
Group Name: ROLE APPROVER FOR BUSINESS PROCESS PR

| <input type="checkbox"/> Approval Expression | Approver | Alternate Approver |
|--|----------|--------------------|
| | | |
| | | |
| | | |
| | | |
| | | |

Change Approval Criteria
Group Name: ROLE APPROVER FOR BUSINESS PROCESS PR

| <input type="checkbox"/> Condition | Attribute | Value |
|------------------------------------|------------------|----------------|
| <input type="checkbox"/> And | Business Process | Procure to Pay |
| | | |
| | | |
| | | |

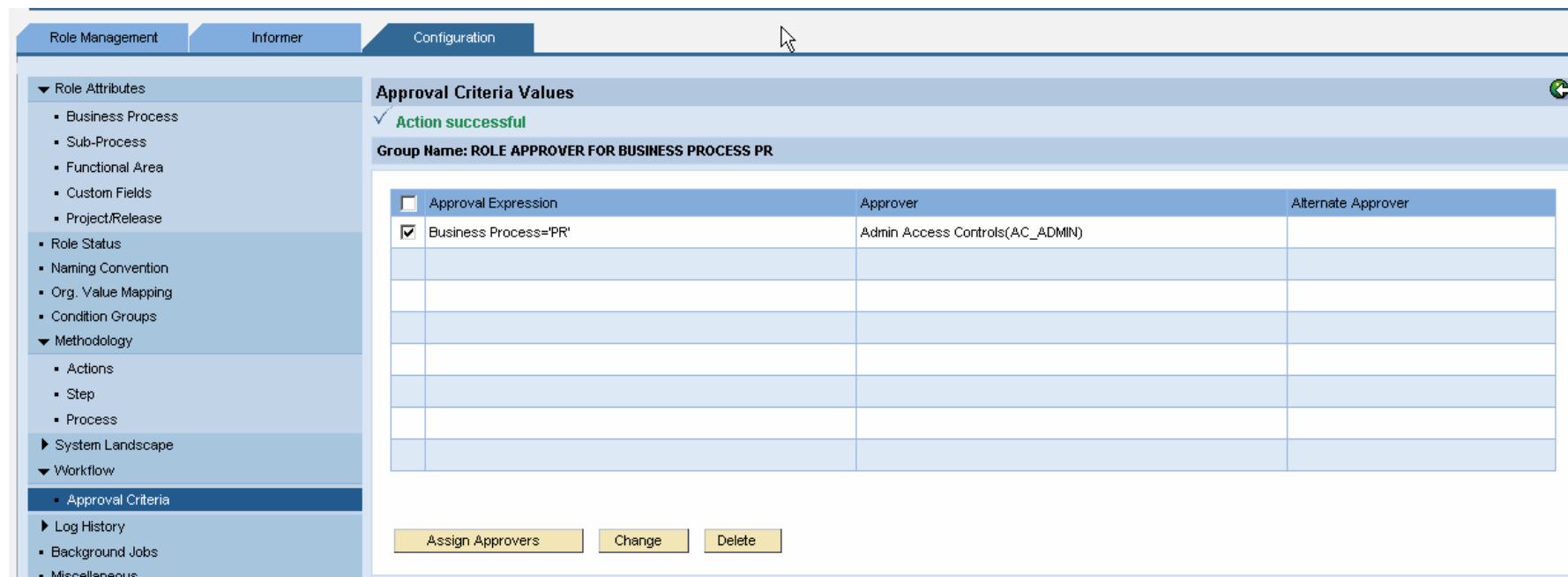
| <input type="checkbox"/> Approver | Alternate Approver |
|-----------------------------------|--------------------|
| <input type="checkbox"/> ac_admin | |
| | |
| | |
| | |

→ **Check Next Slide!**

9 – Definition of Approval Criteria (3/3)



- The result is a list of business processes, each one assigned with a approver and optionally an alternate approver. In our example the list has only one item.
- To these approvers CUP will send approval requests in the role approval step of the methodology process to.



The screenshot shows the SAP Role Management Configuration interface. The left sidebar contains a navigation tree with categories like Role Attributes, Role Status, Methodology, System Landscape, Workflow, and Approval Criteria. The main area is titled 'Approval Criteria Values' and displays a confirmation message 'Action successful' and the group name 'ROLE APPROVER FOR BUSINESS PROCESS PR'. Below this is a table with columns for 'Approval Expression', 'Approver', and 'Alternate Approver'. One row is populated with the expression 'Business Process='PR'' and the approver 'Admin Access Controls(AC_ADMIN)'. At the bottom, there are buttons for 'Assign Approvers', 'Change', and 'Delete'.

| <input type="checkbox"/> Approval Expression | Approver | Alternate Approver |
|---|---------------------------------|--------------------|
| <input checked="" type="checkbox"/> Business Process='PR' | Admin Access Controls(AC_ADMIN) | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

10 – Definition of Naming Conventions



- Create naming Conventions for single, composite & derived roles as well as for profile in your different system landscapes and determine whether the naming convention shall be enforced (recommended).

The screenshot shows the SAP Role Management Configuration interface for defining naming conventions. The left sidebar lists various configuration options, with 'Naming Convention' selected. The main area is titled 'Change Naming Convention' and displays a success message: 'Naming convention saved successfully'. Below this, the configuration details are shown:

- Name***: NAMING CONVENTION ERP SINGLE ROLE
- System Landscape***: ERP SAP Landscape
- Role Type***: Single
- Enforced***: Enabled

The 'Naming Convention' section includes:

- Expression**: A text field containing the pattern: `$$$$_$$_$$$$_#####`
- Attribute**: A dropdown menu set to 'Free Text', with an unchecked checkbox for '(No. of Characters)' and a plus icon.
- Text**: A text input field with a plus icon.
- Maximum No. of Characters**: 30
- Characters Available**: 0
- Table**: A table listing character positions and their descriptions.

| <input type="checkbox"/> | Position | Description |
|--------------------------|----------|-------------------|
| <input type="checkbox"/> | 1-4 | Project/Release |
| <input type="checkbox"/> | 5-5 | User Defined Text |
| <input type="checkbox"/> | 6-7 | Business Process |
| <input type="checkbox"/> | 8-8 | User Defined Text |
| <input type="checkbox"/> | 9-12 | Sub-Process |

A 'Save' button is visible at the bottom left of the configuration area.

11 – Definition of Organization Value Mapping



- Create an example Organizational Value Mapping to have it later available to test the role derivation feature. However, as of AC 5.3 you can also derive roles without org value mappings.
- The idea here is that a primary organizational level exists, which other organizational levels in the same business context depend from.
- Example: A Company may have a business unit for central European region having company codes 1000 to 2000. The org level *Purchasing Org.* depends on the values of CC: Purch. Org. 1000 belongs to the range 1000 – 2000 of CCs. It can be mapped to these values.

Change Org. Value Mapping

Mapping Name* BU CENTRAL EUROPE

Derived Org. Level* Company Code (BUKRS)

Org. Value From* 1000

Org. Value To 2000

Description Countries: GER, F, NL, BEL, LUX, AU, CH

Mapped Org. Levels

| Field | From | To | |
|--|------|----|---|
| <input type="checkbox"/> Purchasing Organization (EKORG) | 1000 | | ➔ |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Save Impacted Master Roles Impacted Derived Roles



- > 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.
- > SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, Duet, Business ByDesign, ByDesign, PartnerEdge 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 and associated logos displayed are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.
- > The information in this document is proprietary to SAP. This document is a preliminary version and not subject to your license agreement or any other agreement with SAP. This document contains only intended strategies, developments, and functionalities of the SAP® product and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development. SAP assumes no responsibility for errors or omissions in this document. SAP does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. 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 shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence.
- > The statutory liability for personal injury and defective products is not affected. 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
- > Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.
- > Einige von der SAP AG und deren Vertriebspartnern vertriebene Softwareprodukte können Softwarekomponenten umfassen, die Eigentum anderer Softwarehersteller sind.
- > SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, Duet, Business ByDesign, ByDesign, PartnerEdge und andere in diesem Dokument erwähnte SAP-Produkte und Services sowie die dazugehörigen Logos sind Marken oder eingetragene Marken der SAP AG in Deutschland und in mehreren anderen Ländern weltweit. Alle anderen in diesem Dokument erwähnten Namen von Produkten und Services sowie die damit verbundenen Firmenlogos sind Marken der jeweiligen Unternehmen. Die Angaben im Text sind unverbindlich und dienen lediglich zu Informationszwecken. Produkte können länderspezifische Unterschiede aufweisen.
- > Die in diesem Dokument enthaltenen Informationen sind Eigentum von SAP. Dieses Dokument ist eine Vorabversion und unterliegt nicht Ihrer Lizenzvereinbarung oder einer anderen Vereinbarung mit SAP. Dieses Dokument enthält nur vorgesehene Strategien, Entwicklungen und Funktionen des SAP®-Produkts und ist für SAP nicht bindend, einen bestimmten Geschäftsweg, eine Produktstrategie bzw. -entwicklung einzuschlagen. SAP übernimmt keine Verantwortung für Fehler oder Auslassungen in diesen Materialien. SAP garantiert nicht die Richtigkeit oder Vollständigkeit der Informationen, Texte, Grafiken, Links oder anderer in diesen Materialien enthaltenen Elemente. Diese Publikation wird ohne jegliche Gewähr, weder ausdrücklich noch stillschweigend, bereitgestellt. Dies gilt u. a., aber nicht ausschließlich, hinsichtlich der Gewährleistung der Marktgängigkeit und der Eignung für einen bestimmten Zweck sowie für die Gewährleistung der Nichtverletzung der geltenden Rechts.
- > SAP übernimmt keine Haftung für Schäden jeglicher Art, einschließlich und ohne Einschränkung für direkte, spezielle, indirekte oder Folgeschäden im Zusammenhang mit der Verwendung dieser Unterlagen. Diese Einschränkung gilt nicht bei Vorsatz oder grober Fahrlässigkeit.
- > Die gesetzliche Haftung bei Personenschäden oder die Produkthaftung bleibt unberührt. Die Informationen, auf die Sie möglicherweise über die in diesem Material enthaltenen Hotlinks zugreifen, unterliegen nicht dem Einfluss von SAP, und SAP unterstützt nicht die Nutzung von Internetseiten Dritter durch Sie und gibt keinerlei Gewährleistungen oder Zusagen über Internetseiten Dritter ab.
- > Alle Rechte vorbehalten.