Faced with a Complex SAP Landscape? Tips and Tricks for Managing and Administering Your GRC Systems

Kurt Hollis
Deloitte Consulting
In This Session (Part 1 – Architecture, Installation, Configuration)

- Review the architectural details and requirements of SAP solutions for GRC 10.1 in a straightforward and easy-to-understand manner
- Properly size the systems based on hardware and software requirements
- Examine how to manage the technical landscape of systems and servers required to make the entire GRC solution function and how they are connected
- Brief discussion on technical implementation
- Review of key points around the upgrade and migration from prior releases of GRC to the latest version
- Review the GRC post-installation steps including setup of Risk Analysis, Emergency Access, and Access Requests
In This Session (Part 2 – Jobs, Performance, Monitoring, Troubleshooting)

- GRC job processing details
- Run and monitor Risk Analysis Jobs and other important Jobs
- Critical information needed to improve the operation and performance of GRC
- Performance of GRC with a focus on Access Control and Risk Management processing
- Dig into some of the key performance issues that can happen
- A focus is on the Rule Set used with GRC Access Control where a good amount of informative detail is discussed
- Performance of the Risk Analysis functions in Access Control is addressed with suggested tips to improve processing
- Monitor the GRC system and become proactive to prevent problems before they occur
- Review a variety of Technical Tips which are based on real experience and which will lead to a better-running GRC system
- Common problems and monitoring of the system is reviewed
What We’ll Cover

- Technical Architecture
- Sizing
- Landscape and Client Strategy
- Implementation
- Upgrade and Migration Important Points
- Post-Installation and Configuration
- Job Processing
- Landscape Connectivity
- Performance
- Technical Tips
- Monitoring
- Wrap-up
SAP GRC Access Control 10.1 Technical Architecture

Note: Red boxes indicate required components

Source: SAP Master Guide
SAP GRC Process Control 10.1 Technical Architecture

Note: Red boxes indicate required components

Source: SAP Master Guide
SAP GRC Risk Management 10.1 Technical Architecture

Source: SAP Master Guide
Technical Architecture — Major Components

- ABAP Stack ➔ SAP NetWeaver® 7.40 SP04 (required) – latest available recommended (currently SP14)
  - SAP NetWeaver ABAP stack is required for GRC 10.1
    - Must be version 7.40
      - GRCFND_A 1100 is compatible with SAP NetWeaver 7.40 SP04 and above (SAP_BASIS)
  - Access Control, Process Control, and Risk Management (as of 10.0 and 10.1) are combined together in one “foundation” component (package)
  - SAP HANA is available is a database choice with the system
  - Optional reporting requires BI content 7.47 (not used often), HANA provides a new reporting platform (HANA Live)
• Plug-ins for SAP ERP and SAP NetWeaver systems (previously called RTA)
  • For Upgrades, previous plug-in components VIRSA, VIRSANH, VIRSAHR, and GRCPCRTA are renamed GRCPINW and GRCPIERP as of 10.0 and 10.1
  • GRC 10.1 plug-ins (GRCPIERP, GRCPINW) are available for SAP ERP, SAP ERP HCM, and SAP NetWeaver systems
  • GRC plug-in release includes backwards support for the AC 5.3 releases (since 10.0 SP4 versions and higher)
    • GRCPIERP V1100_700 for ERP 6.0 EHP1-7+
    • GRCPINW V1100_700 for 7.00, 7.02, 7.03, 7.0x systems
    • GRCPINW V1100_710 for 7.10 and 7.30 systems
    • GRCPINW V1100_731 for 7.31 and 7.40 systems
• Non-SAP ERP systems can also be connected via adapters from Greenlight Technologies
Technical Architecture — Major Components (cont.)

- Java Stack ➔ SAP NetWeaver 7.02 EHP2 or 7.30/7.31 or 7.40 (optional, but recommended)
  - SAP NetWeaver 7.0x/7.3x/7.40 Java stack is required for Adobe Document Services
    - Must include the WD ALV List Viewer Component for Web Dynpro-based reports and PDF viewing and printing (BI Java Usage type needed)
  - Optionally, if you want the SAP Enterprise Portal for your front end for GRC applications, you must have an SAP NetWeaver 7.02/7.31/7.40 Java Stack with Portal usage types installed
    - Additionally, the GRC Portal “business” package needs to be deployed in the portal system
Architecture Expert Tips

• Do not combine the GRC ABAP components on existing SAP NetWeaver systems running other SAP business solutions or SAP Solution Manager systems

• Standalone ABAP stack installation recommended for the GRC components (do not use an upgraded ABAP+JAVA dual stack)

• If Portal/Java optional part is needed, install the Java stack along with the needed usage types (such as usage type EP/BI)
  • However, this is not required if one is already available in the landscape which meets the requirements for version, sizing, and software lifecycle strategy

• Java stack is required for Adobe Document Services if PDF support is required and must include the WD ALV List Viewer component for Web Dynpro-based reports and PDF viewing and printing (Portal and BI Java usage types needed)

• SAP Enterprise Portal is optional, as stated before
NEW — Setup for Integration with SAP HANA

• (1) HANA system or have GRC installed on a HANA Database
• (2) HANA Live GRC Analytics add-on
• (3) May use the SLT (Replication software) to get the data into HANA for Analytics reporting
• (4) Replication will create the tables in HANA for reporting
• (5) Views are created for reporting (see: [http://help.sap.com/hba](http://help.sap.com/hba) and find SAP HANA Live for SAP solutions for GRC in the list)
NEW — Smart Business 1.0 for Access Control Management

- SAP Smart Business 1.0 for Access Control Management is an SAP Smart Business cockpit that provides you with an overview of the most important key performance indicators for an access control administrator (see: http://help.sap.com/ssb)
- This package combines Fiori application with Reporting capabilities
- Reports:
  - Access Requests by Stage
  - Access Requests via Escape Path
  - All Access Requests
  - Critical Profile Assignments
  - Critical Role Assignments
  - Failed Access Provisioning
  - Firefighter Usage
  - Frequently Used Actions
  - Frequently Used Roles
  - Open Access Requests
  - Role Analytics
  - Role Assignment Efficiency
  - Roles Available
  - Roles with Unmitigated Risks
  - Unassigned Roles
  - User Accounts Available
  - Users with Unmitigated Risks
  - Violations Performed
Java Components

- The SAP Java Components for 10.0 SP11 are reused for SAP solutions for GRC 10.1
- GRC 10.1 supports the following SAP NetWeaver versions for SAP JAVA components:
  - SAP Portal Plug-In: SAP NetWeaver 7.00, 7.02, 7.30 – SP11, 7.31 – SP07, and 7.40 – SP02
  - SAP Portal Content: SAP NetWeaver 7.02, 7.30 – SP11, 7.31 – SP07, and 7.40 – SP02
- Use the following compatibility matrix to determine the versions of SAP NetWeaver, SAP Portal Plug-In, and SAP Portal Content that work together:

<table>
<thead>
<tr>
<th>SAP NetWeaver Version</th>
<th>SAP Portal Plug-In Version</th>
<th>SAP Portal Content Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.00</td>
<td>7.00</td>
<td>N/A</td>
</tr>
<tr>
<td>7.02</td>
<td>7.00</td>
<td>7.02</td>
</tr>
<tr>
<td>7.30 - SP11</td>
<td>7.30</td>
<td>7.02</td>
</tr>
<tr>
<td>7.31 - SP07</td>
<td>7.30</td>
<td>7.02</td>
</tr>
<tr>
<td>7.40 - SP02</td>
<td>7.30</td>
<td>7.02</td>
</tr>
</tbody>
</table>
GRC 10.1 User Interface BC
SAP GRC 10.1 Front End — User Interface

- Three methods for user interface:
  - Use common web browser to access the “embedded” BC to access the role-based menus for the GRC applications
  - SAP Enterprise Portal to access all GRC solutions (Portal requires the GRC Business Package installed)
  - BC 3.0/3.5/4.0 installed on the client PC or laptop
- SAP GUI 7.30 (older, out of support) and 7.40 (newer) is only needed for administrators and implementation team
- Adobe Document Services provides PDF support
- Adobe Flash Player 10 provides dashboards
- Crystal Adapter is required for viewing GRC Crystal reports
- Fiori is an Enhancement Option to the User Interface
SAP GRC 10.1 Front End — Portal Facts

- SAP Enterprise Portal 7.02/7.3x./7.40 can be used optionally
- GRC Portal content contains the GRC Portal UI elements to access the GRC suite
- Portal’s AS Java can contain an Adobe Document Services instance; in effect, Portal and ADS may be shared on one AS Java instance
- AC/PC/RM 10.1 requires the add-on portal business package GRC_POR and the software component BP ERP05 Common Parts version 1.51
- Versions 7.02-7.31 use the 7.02 Plug-In
- Version 7.31 and 7.40 use the 7.31 Plug-In
SAP GRC 10.1 — New Fiori User Interface

- Fiori Component is available for GRC 10.1 and is based on SAP NetWeaver 7.31 and 7.40 with GRC 10.1
- Requires ADD-ON Component ➔ FIORI FOR SAP GRC 1.0 (SP06 it was available)
- GRC component must be 10.1 SP08 or newer
- To install SAP Fiori product and implement the contained apps the system landscape must be set up to enable SAP Fiori first
- Typically set up the required gateway and the UI5 OData locally in the GRC system
- Follow the steps at http://help.sap.com/fiori_bs2013 to configure the Fiori Launchpad
- Supports the HANA database with the same Fiori application setup
What We’ll Cover

- Technical Architecture
  - Sizing
- Landscape and Client Strategy
- Implementation
- Upgrade and Migration Important Points
- Post-Installation and Configuration
- Job Processing
- Landscape Connectivity
- Performance
- Technical Tips
- Monitoring
- Wrap-up
Hardware and Sizing

- Follows the same platform considerations for all SAP NetWeaver-based systems
- Refer to Product Availability Matrix (PAM) and release strategy
- Can use a variety of hardware, operating systems, and databases:
  - IBM running AIX, i5/OS, or z/OS with DB2 database
  - HP with HP-UX with Oracle database
  - Sun with Solaris with Oracle database
  - SUSE or Red Hat Linux on a variety of hardware platforms
  - MS Windows Servers (64-bit OS) with MS SQL database
- Unicode and 64-bit only installation supported
- SAP HANA is now supported as Database for GRC 10.1
• Large systems (with multiple application servers) are not normally required for SAP GRC solutions
  † Suggestion: Pick a platform that SAP has a long support lifecycle for and that your company is trained and confident in
• Server size, CPU, and memory
  † ABAP Web Dynpro requires more memory than typical apps; therefore, 16GB memory minimum suggested for good performance
  † Batch jobs for risk analysis require more CPU and memory — suggest two CPU cores minimum and 16GB memory
• Database space: Initial 100-200GB, plus yearly growth (see sizing)
• Additional space required for AC risk analysis data, which can start at 20GB and extend up to 200GB for the main tables!
### Sizing Guidelines Example — Access Control 10.1

#### User Synchronization

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Peak Memory (MB)</th>
<th>Minimum Disk Space (MB)</th>
<th>Minimum SAPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>Synchronize 5000 users</td>
<td>4</td>
<td>327</td>
<td>2500</td>
</tr>
<tr>
<td>Medium</td>
<td>Synchronize 10,000 users</td>
<td>4</td>
<td>210</td>
<td>5000</td>
</tr>
<tr>
<td>Large</td>
<td>Synchronize 15,000 users</td>
<td>4</td>
<td>1,490</td>
<td>7500</td>
</tr>
</tbody>
</table>

#### Role Synchronization

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Peak Memory (MB)</th>
<th>Minimum Disk Space (MB)</th>
<th>Minimum SAPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>Synchronize 1000 roles*</td>
<td>8</td>
<td>2.67</td>
<td>1000</td>
</tr>
<tr>
<td>Medium</td>
<td>Synchronize 3000 roles*</td>
<td>8</td>
<td>6.24</td>
<td>3000</td>
</tr>
<tr>
<td>Large</td>
<td>Synchronize 5000 roles*</td>
<td>8</td>
<td>6.87</td>
<td>5000</td>
</tr>
</tbody>
</table>

#### User Risk Analysis

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Peak Memory (MB)</th>
<th>Minimum Disk Space (MB)</th>
<th>Minimum SAPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>1 user*</td>
<td>68</td>
<td>0.005</td>
<td>10</td>
</tr>
<tr>
<td>Medium</td>
<td>10 concurrent users*</td>
<td>68</td>
<td>0.045</td>
<td>100</td>
</tr>
<tr>
<td>Large</td>
<td>25 concurrent users*</td>
<td>68</td>
<td>0.110</td>
<td>250</td>
</tr>
</tbody>
</table>

#### Role Risk Analysis

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Peak Memory (MB)</th>
<th>Minimum Disk Space (MB)</th>
<th>Minimum SAPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>1 user*</td>
<td>64</td>
<td>0.005</td>
<td>10</td>
</tr>
<tr>
<td>Medium</td>
<td>10 concurrent users*</td>
<td>64</td>
<td>0.045</td>
<td>100</td>
</tr>
<tr>
<td>Large</td>
<td>25 concurrent users*</td>
<td>64</td>
<td>0.110</td>
<td>250</td>
</tr>
</tbody>
</table>
Sizing Guidelines Example — Access Control 10.1 (cont.)

Batch User Risk Analysis

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Peak Memory (MB)</th>
<th>Minimum Disk Space (MB)</th>
<th>Minimum SAPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>1000 users</td>
<td>4</td>
<td>125</td>
<td>2000</td>
</tr>
<tr>
<td>Medium</td>
<td>5000 users</td>
<td>8</td>
<td>625</td>
<td>10,000</td>
</tr>
<tr>
<td>Large</td>
<td>10,000 users</td>
<td>8</td>
<td>1,250</td>
<td>20,000</td>
</tr>
</tbody>
</table>

Batch Role Risk Analysis

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Peak Memory (MB)</th>
<th>Minimum Disk Space (MB)</th>
<th>Minimum SAPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>100 roles*</td>
<td>8</td>
<td>98</td>
<td>400</td>
</tr>
<tr>
<td>Medium</td>
<td>1000 roles*</td>
<td>8</td>
<td>978</td>
<td>4000</td>
</tr>
<tr>
<td>Large</td>
<td>5000 roles*</td>
<td>20</td>
<td>4,892</td>
<td>20,000</td>
</tr>
</tbody>
</table>

Access Request Analysis

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Peak Memory (MB)</th>
<th>Minimum Disk Space (MB)</th>
<th>Minimum SAPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>1 user creating a request*</td>
<td>45</td>
<td>0.1</td>
<td>15</td>
</tr>
<tr>
<td>Medium</td>
<td>10 concurrent users each creating one request*</td>
<td>53</td>
<td>0.98</td>
<td>150</td>
</tr>
<tr>
<td>Large</td>
<td>25 concurrent users each creating one request*</td>
<td>53</td>
<td>2.45</td>
<td>375</td>
</tr>
</tbody>
</table>

- Access Control’s most intensive operation is Risk Analysis at around 10,000 SAPS
- Process Control SAPS are typically below 1,000 for 100 users per operation
- The Disk Space estimates provided in these charts do not take into account storage for Risk Analysis data
What We’ll Cover

- Technical Architecture
- Sizing
- Landscape and Client Strategy
  - Implementation
  - Upgrade and Migration Important Points
  - Post-Installation and Configuration
  - Job Processing
  - Landscape Connectivity
  - Performance
  - Technical Tips
  - Monitoring
  - Wrap-up
SAP GRC 10.1 Landscape Considerations

- Development, QA (Test), and Production is recommended (three-system landscape)
  - However, a two-system landscape has been implemented by some customers
- 10.1 supports multiple client setup in the ABAP stack
- If using Portal, the Portal connector can point to only one GRC ABAP client at a time
  - It is possible to set up duplicate Portal content, roles, and additional connectors for supporting multiple clients from Portal
Example of SAP GRC 10.1 Client Strategy
What We’ll Cover

• Technical Architecture
• Sizing
• Landscape and Client Strategy

• Implementation
• Upgrade and Migration Important Points
• Post-Installation and Configuration
• Job Processing
• Landscape Connectivity
• Performance
• Technical Tips
• Monitoring
• Wrap-up
Resources Required

• Technical Team – Basis skills
  • SAP NetWeaver ABAP and Java installations
  • SAP Enterprise Portal Installation
  • Adobe Services (for PDF reporting)
  • SAP Business Workflow (BRF+) setup (important skill needed)
  • Email integration
  • SAP BW setup and integration (optional)
  • HANA and Fiori experience may be needed if to be used
  • Mobility experience if mobile is to be used
• Functional Team – Skills
  • Configuration, SOD Analysis, and SAP Security for SAP AC
  • Configuration and Business Processes for SAP Process Control and Risk Management
  • Configuration and Business Processes for SAP Global Trade Services
• Security
  • ABAP and Java roles
### Installation Planning

- **Nine-step, high-level plan to implement GRC Suite 10.1**

<table>
<thead>
<tr>
<th>STEP</th>
<th>Description</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Project plan, review guides, and SAP Notes for installation and download software. Verify server readiness, O/S, and patches and that users for O/S access to the system are set up.</td>
<td>1 day</td>
</tr>
<tr>
<td>2</td>
<td>SAP technical team installs SAP NetWeaver ABAP 7.40 and optional Java system(s). Installation includes database system and required patches (New system installation).</td>
<td>2 days</td>
</tr>
<tr>
<td>3</td>
<td>Install support packages for SAP NetWeaver (SP01-SP0x)</td>
<td>.5 day</td>
</tr>
<tr>
<td>4</td>
<td>Install SAP GRC applications and required support packages (GRCFND_A Package and SP01-SP0x). See SAP Note 1490996. Use SAINT to install.</td>
<td>.5 day</td>
</tr>
<tr>
<td>5</td>
<td>Install GRC Plug-in component in SAP ERP back-end system (GRCPIERP, GRCPINW). Use SAINT to install. See SAP Notes 1500689 and 1500690.</td>
<td>.5 day</td>
</tr>
</tbody>
</table>
Installation Planning (cont.)

<table>
<thead>
<tr>
<th>STEP</th>
<th>Description</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Perform all technical post-step configurations:</td>
<td>2 days</td>
</tr>
<tr>
<td></td>
<td>• ABAP parameter changes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Set up clients, activate apps, activate SICF, activate BCSETS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Set up STMS, ICM, SSO, SSL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Licenses, backups, monitoring</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Perform all SAP GRC application (technical-related) post-step configurations</td>
<td>1-2 days</td>
</tr>
<tr>
<td>8</td>
<td>Perform quality checks for installation, performance considerations</td>
<td>.5 day</td>
</tr>
<tr>
<td>9</td>
<td>Perform go-live checks (SAP) (Production systems only)</td>
<td>1 days</td>
</tr>
</tbody>
</table>

- Six to seven days is typical for SAP NetWeaver and GRC installation, but varies based on skills.
- Experienced GRC person can complete in one week with some tasks done in parallel.
What We’ll Cover

• Technical Architecture
• Sizing
• Landscape and Client Strategy
• Implementation

• Upgrade and Migration Important Points
• Post-Installation and Configuration
• Job Processing
• Landscape Connectivity
• Performance
• Technical Tips
• Monitoring
• Wrap-up
SAP GRC 10.0/10.1 Upgrade Paths

Access Control
JAVA
5.2
Upgrade
ABAP
4.0
5.3

Risk Management
ABAP
2.0
Upgrade

Process Control
ABAP
2.5
3.0

Global Trade Services
ABAP
7.0
7.1
7.2
8.0

Nota Fiscal Electronica
ABAP
1.0
2.0

GRC v10.0 Suite
Access Control
Risk Management
Process Control
Global Trade Services
Nota Fiscal Electronica

Source: SAP
Access Control 10.1 Migration Overview

- SAP provides a migration tool with capability to export data from existing Access Control 4/5.3 to Access Control 10.1
- Java-based versions 5.2/5.3 cannot be upgraded directly to ABAP-based version 10.1 due to the difference in platform
- The migration tool provides the following functionalities:
  - Automated process with limited manual effort
  - Ability to transfer configuration data, which includes SAP connectors, RAR configuration parameters, ERM configuration parameters, as well as CUP configuration parameters
  - Export master data, including user roles and rule sets
  - Ability to export data onto a spreadsheet and customize it before import
  - Flexibility to filter and modify data before export
Access Control Migration Checklist

- Ensure SAP NetWeaver is at least 7.0 SP11 and AC 5.3 SP13
- Access Control 5.2 will first need to be upgraded to version 5.3
- Complete the configuration in IMG for the SAP connectors and new components
  - Refer to the GRC 10.1 Configuration Guide for more information
- Create appropriate owners/users within Access Control 10.1
- Create the appropriate Org. Unit to import the RAR data
- Before migrating CUP and ERM data, manually create all AC 5.3 custom fields in GRC 10.1 using identical names
- Activate Business Configuration Sets (BCSETS) for 10.1 based on details in the migration guide
- Upgrade the RTA in the ERP back end to the new GRC 10.1 plug-ins
GRC 10.0/10.1 Access Control Data Migration Process

- Export the RAR and SPM data (AC 4.0) or export the SPM data (AC 5.3)
- Export the CUP, RAR, and ERM data (AC 5.3 only)
- Exporting AC 5.3 (CUP/RAR/ERM) data
- Complete the import prerequisites for data import
- Import the data into GRC 10.0/10.1
- Complete the post-import tasks
  - Set up BRF+ rules (ABAP functions)
    - These replace the CUP initiators and custom approver determinators, ERM role approver criteria, and condition groups for methodologies
  - Creation of email templates
What We’ll Cover

• Technical Architecture
• Sizing
• Landscape and Client Strategy
• Implementation
• Upgrade and Migration Important Points
• Post-Installation and Configuration
• Job Processing
• Landscape Connectivity
• Performance
• Technical Tips
• Monitoring
• Wrap-up
GRC 10.1 Implementation – Technical Post Steps

1. Bring System up and Login to the System
2. Verify the Client Copy is Completed
3. Activate Applications in Client
4. Maintain Web Services in SMICM (HTTP)
5. Workflow Setup
6. Test NWBC user Interface
7. New UI5 Odata Services
8. STRUST SSO Setup
9. EMAIL Setup
10. System Connections Setup
SPRO — Initial Configuration and Setup

- Perform the GRC Setup and Configuration in “SPRO” (IMG)
Step 1: Client Setup — Key Points

- Two methods to set up client (see SAP Note 1505255 – GRC 10.1)
  - Install the software and then copy client 000 using parameter “sap_all” to the new client (preferred for new system)
  - If client exists and you need to move only the client-specific data, use “Copy through the Customizing Piece List Transport” option to bring only SAP GRC 10.1 client-specific data from client 000 to the specified target client
    - Transaction SCC1
    - Use Piece List Transport
    - SAPK-V10AGINGRCFNDA
    - Copy using Client-Specific Objects option
    - Needed for PC/RM, but not needed for AC
Step 2: Activate Applications

- Activate the applications in SPRO (IMG)
Step 3a: SMICM/HTTP Setup — Key Points

- GRC suite 10.1 is based on ABAP Web Dynpro technology; therefore, they are pure web-based applications
- Set up web services in the ABAP stack using SMICM
  - Set up HTTP and HTTPS server ports
  - Create profile parameters in RZ10
- Set time-out values high enough for users not to experience session terminations
  - Example below allows one hour

```plaintext
icm/server_port_0 PROT=HTTP,PORT=80$$,TIMEOUT=3600,PROCTIMEOUT=1800
```

<table>
<thead>
<tr>
<th>No.</th>
<th>Log</th>
<th>Service Name/Port</th>
<th>Host Name</th>
<th>Keep Alive</th>
<th>Proc.TimeOut</th>
<th>Actv</th>
<th>External</th>
<th>Bind</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HTTP</td>
<td>8000</td>
<td>socwe1er37.solution</td>
<td>3.000</td>
<td>1.800</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>HTTPS</td>
<td>8260</td>
<td>socwe1er37.solution</td>
<td>3.000</td>
<td>1.800</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>SMTP</td>
<td>0</td>
<td>socwe1er37.solution</td>
<td>30</td>
<td>60</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 3b: ICF Activation — Key Points

- Specific Internet Communication Framework (ICF) public and Web Dynpro services have to be activated
  - Use transaction SICF to activate
- They may become inactive by default after installation or SP upgrade
- Activate selected or all ICF services within:
  - /sap/public
  - /sap/bc
  - /sap/grc
  - /sap/opu
- See SAP Install guide for list of them
Step 3c: ICF Activation — Tip

- Suppress the BC launch selection window; deactivate this service if desired (optional)
Step 3d: SSO Trust Manager Setup

- Using transaction STRUSTSSO2, activate the PSE and SSL
Step 4a: SAP Business Workflow Set-Up Steps

- Use steps in IMG to activate and set up workflow
  - Perform Automatic Workflow Customizing
  - Perform Task-Specific Customizing
Step 4b: SAP Business Workflow Set-Up Steps

- Use steps in IMG to activate and set up workflow
  - Execute RS_APPL_REFRESH using transaction SE38/SA38 (needed to get the entries to appear the first time)
  - Perform task-specific customizing (IMG) (set all TSxxxx to general task)
  - Set Event Linkage details (must activate event linkage) and set error feedback to “Do not change linkage”
  - Event Queue “SWEQADM” (optional for performance needs)
Step 4c: SAP Business Workflow Set-Up Steps

- With a Plugin installed in the GRC system, must use transaction PFTC
  - Set the Tasks to “General Task”
- Use transaction SWDD to activate the workflows (not shown)
Step 5: Email Setup

- Transaction SCOT
- Set up SMTP connection to company’s email gateway and schedule the mail send job
- Extended notification of SAP business workflow for email notifications, reminders, and escalations can also be configured in SPRO
- User’s email address must be maintained in the user’s records (SU01)
Step 6a: Set Up SAP Gateway and OData for New UI5 Interface

1. Set up and activate the SAP Gateway Connection
2. Activate and maintain the services
Step 6b: Set Up SAP Gateway and OData for New UI5 Interface

- Required for the new Access Control Request screens in the BC and the Remediation View User Risk Analysis
- Configure the SAP Gateway and services in SPRO for new access request screens
Step 7a: Deploy Portal Packages (Optional) Key Points

- Deploy these Portal packages:
  - BP_ERP05_COMMON_PARTS (version 1.51)
  - GRC_POR (contains all parts)

- Connectors must be maintained for Access Control, Process Control, Risk Management to connect to the GRC ABAP system

- Aliases for the system names mandated: SAP-GRC and SAP-GRC-AC (Access Control), SAP-GRC-PC (Process Control), and SAP-GRC-RM (Risk Management)

- Portal roles “GRC_SUITE” must be assigned to the users
  - Recommended to use groups to make it easier to manage
    - Assign ERP_COMMON to everyone in this new group
    - Each application has additional roles to be assigned
Step 7b: Deploy Portal Packages (Optional) Key Points

- SSO must be set up
  - Import the Portal certificate into the GRC suite 10.1 ABAP system
- It is required to delete the existing Process Control/Risk Management content from the Portal prior to deploying new support packages
- This may require steps to set up custom worksets and iViews again
- Procedure to add additional regulation types must be completed again
Step 8: Implementation — Plug-In Connection

- AC 10.0/10.1 plug-ins will upgrade any existing RTA from previous AC releases
- Co-existence with AC 5.3 exists with SP04 and higher of the plug-in
- Connectors use RFC configuration to connect to other SAP systems
- No need for SAP JCo connectors any more with AC 10.1
- Connectors are assigned in the IMG (SPRO) for the GRC applications to use
- Transaction is GRPCRTA_PC to set up connector for Process Control in the ERP system side
GRC 10.1 Risk Analysis Configuration

Activate BC Sets (Rule Sets) → Run the Full Batch Risk Analysis → Run the Batch Risk Analysis Monitor
Generate the Rules → Test Risk Analysis
Maintain Configuration Settings for ARA → Run the Synchronization Jobs

Run the Risk Violation Dashboards → Check the Application Logs SLG1
Step 1a: BC Sets — Key Points

- Business Configuration (BC) Sets are an official implementation toolset used to simplify the customization process.
- There are certain BC Sets that are delivered with GRC suite 10.1 that need to be activated.
  - Transaction SCPR20
  - Perform the activation in Development “Config” client
    - Transports will be created
    - Move these transports up the landscape (and also to other Development clients)
- Errors may occur during the activation (see SAP guide).
  - BC Sets that begin with GRPC-ATTR-* have errors that can be ignored.
  - These are documented in SAP Notes and guides.
Step 1b: Configure Rule Sets

- GRC 10.1 rule set is delivered with BC Sets
  - Activate the rules BC Set with transaction SCPR20
- An alternative to BC Sets, you also can upload rules from SPRO
  - SPRO ➔ Governance, Risk, and Compliance ➔ Access Control ➔ Access Risk Analysis ➔ SOD Rules ➔ Upload Rules (use the same files as delivered for Access Control 5.3 rule files)
- SOD rule files (nine) can be uploaded into the AC 10.1 system using transaction code GRAC_UPLOAD_RULES with Append/Overwrite option
- AC 10.1 SOD action rules can be validated by looking at the table GRACACTRULE
- For the other tables related to SOD rules, click F4 to see dropdown of the *GRAC*RUL* tables from transaction SE16
- NOTE: For Process Control use cases ➔ The Master Data Load Utility formally called MDUG is now built into the system and accessed using transactions
Step 1c: BC Sets — Key Points

- Activation is done using SCPR20
- New Rules are loaded using this method
- All initial configuration is loaded using this method (loading is client-specific)

Analysis

<table>
<thead>
<tr>
<th>BC Set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRAC_RA_RULESET_COMMON (THIS ONE)</td>
<td>SOD Rules Set</td>
</tr>
<tr>
<td>GRAC_RA_RULESET_SAP_BASIS (NO)</td>
<td>SAP Basis Rules Set</td>
</tr>
<tr>
<td>GRAC_RA_RULESET_SAP_HR (NO)</td>
<td>SAP HR Rules Set</td>
</tr>
<tr>
<td>GRAC_RA_RULESET_SAP_NHR</td>
<td>SAP R/3 less HR Basis Rules Set (Not needed)</td>
</tr>
<tr>
<td>GRAC_RA_RULESET_SAP_R3 (THIS ONE)</td>
<td>SAP R/3 AC Rules Set</td>
</tr>
<tr>
<td>GRAC_RA_RULESET_SAP_SRM (NO)</td>
<td>SAP SRM Rules Set</td>
</tr>
</tbody>
</table>

Specific to Access Request Management

- GRAC_ACCESS_REQUEST_REQ_TYPE*: Request Type
- GRAC_ACCESS_REQUEST_EUP*: EUP (Note: Only the value EU ID 999 is valid for this BC set)
- GRAC_ACCESS_REQUEST_APPL_MAPPING*: Mapping BRF Function IDs and AC Applications
- GRAC_ACCESS_REQUEST_PRIORITY*: Request Priority

Specific to Business Role Management
Step 2: Generate the SOD Rules

- Using the SPRO IMG, Generate the SOD Rules for the first time
Step 3: Maintain Configuration Settings

- Maintain Configuration Settings. Use SPRO to review the configuration settings.
- FYI – SAP has a guide dedicated to the configuration settings available for download
Step 4: Check and Maintain Rules

- Enter into the BC to check and maintain the rules
- Check the Access Risks, Functions, and Rule Set
Quick Info – Synchronization Jobs in GRC 10.1

- Synchronization jobs can be run from SPRO IMG and navigating to Governance, Risk & Compliance > Access Control > Synchronization Jobs
  - Authorization Synch – Synchronizes PFCG Authorization data
  - Repository Object Synch – Synchronizes Profiles, Roles, and Users master data
  - Action Usage Synch – Synchronizes action usage data
  - Role Usage Synch – Synchronize role usage data
  - Firefighter Log Synch – Synchronizes the firefighter logs from plug-in system to GRC system
  - Firefighter Workflow Synch – Initiates FF log report review workflow based up on your workflow settings which sends the FF log report to FF controller for review
  - EAM Master Data Synch – This is the new job introduced as part of De-centralized firefighting. Synchronizes the EAM data from GRC box to Plug-in system. Once you have created all required users execute this job to synchronize the data from GRC to plug-in system.
Step 5a: Perform Synchronization Jobs

- In IMG, go to Access Control → Synchronization Jobs and run Authorization Sync (program GRAC_PFCG_AUTHORIZATION_SYNC). It is recommended to run it in the background. This program contains three jobs: Org. Value sync, Transaction Sync, and Objects sync.
Step 5b: Repository Object Sync

- Repository Object Sync (program GRAC_REPOSITORY_OBJECT_SYNC)
- Perform a full sync
- On larger systems with many users and roles, this job may take 10-20 minutes to run
- NOTE: These jobs can be scheduled to run in background using SM36 to create the background job and SE38 to create the variants to store the values in the fields so they can be used over and over again. Usually, a full sync is done weekly and an incremental sync is done daily. More frequent jobs can be scheduled to allow new users and roles to be used in the GRC analysis jobs, reports, and ad hoc analysis.
Step 6a: Run Batch Risk Analysis

- Set up and run the Initial Batch Risk Analysis using SPRO → Execute Batch Risk Analysis
Step 6b: Verify the Risk Analysis Results

- From the BC Report menus ➔ Access Risk Violations
- The following screen should open up
Emergency Access Configuration

1. Activate BC Sets (Emergency Access)
2. Add Connectors to Firefighting Scenario (SUPMG)
3. Maintain Configuration Settings
4. Maintain Criticality Levels
5. Assign Firefighter IDs to Firefighters
6. Define Owners and Controllers
7. Complete Synchronization
8. Create Firefighter IDs in Target Systems
9. Access Firefighter ID
10. Run Log Collection Job
11. Access and Review Firefighter Logs
Step 1 – Activate the BCSET for EAM

- BC Set Activation using SCPR20 to perform the load and activation of the GRAC_SPM_CRITICALITY_LEVEL
Step 2 – Plug-In Configuration Settings

- Add the configuration in the Plug-In system for the FFID Role name to be used
Step 3 – Setup Connector for EAM

- Setup connector specific setting in the IMG (SPRO)
- Enter into the integration scenario settings shown below
- Enter SUPMG in integration scenario and assign the target connector
Step 4 – Set the EAM Critical Levels and Parameters

- Enter the criticality levels for Emergency Access Management using SPRO and IMG.
- Enter the configuration settings and parameters for EAM using SPRO and IMG.
Tip – FF Users and Roles

- **FF_OWNER User** – Owner for the firefighter ID. Assign the role
  Z_SAP_GRAC_SUPER_USER_MGMT_OWNER.

- **FF_CONTROLLER User** - Firefighter Controller. Assign the role
  Z_SAP_GRAC_SUPER_USER_MGMT_CNTLR. (Verify valid email address is maintained in
  SU01 to receive notifications via email)

- **FIREFIGHTER User** – Firefighter user who will be able to access in the target system with
  the Firefighter ID. Assign Z_SAP_GRAC_SUPER_USER_MGMT_USER in addition to the
  base roles. Note: Without the base role you will not see the Firefighter user available for
  selection in the Firefighters IDs.

<your user> – User performing the configuration. Must have the role
Z_SAP_GRAC_SUPER_USER_MGMT_ADMIN assigned.

- All users must have the roles Z_SAP_GRAC_NWBC and Z_SAP_GRAC_BASE assigned.
Tip – Centralize and De-Centralized Firefighter

- SAP has enabled de-centralized firefighting feature in GRC 10.0 from SP10 release.
- Depending on the needs, the option “log on centrally” (current version 10 behavior) or “log on locally” (5.3 behavior) can be configured in GRC 10 and GRC 10.1.
- The system has the ability where both centralized and de-centralized approach can be configured but user can either login centrally or locally as there can be only one firefighter session at a time.
Step 5 – Create Firefighter IDs and Synchronize Users

- Create the Firefighter IDs in SU01 in target system
- Assign corresponding roles required roles/profiles according to your requirements. Must assign to the FIREFIGHTER_ID the role Z_SAP_GRC_SPM_FFID (copied from SAP role).
- This user should be of type “Service” (refer to SAP Note 1702439)
- Synchronize created Firefighter IDs using T-code GRAC_REP_OBJ_SYNC
Step 6 – Define the Owners and Controllers

- Define Owners and Controllers for the created Firefighter ID in BC
- Assign Firefighters to Owners
Step 7 – Define the Reason Codes

- Reason Codes are created and maintained in GRC system using BC → Setup → Maintain Reason Code assignments
- Add the Reason Code and a long description within the respective text fields
- To define the systems for which the created reason code is applicable, click add within the system table
Using Firefighter

- FF Users execute Tcode /n/GRCPI/GRIA_EAM in the Plug-in system and login with firefighter IDs assigned to them (Decentralized)
- The role SAP_GRAC_SUPER_USER_MGMT_USER must be assigned to the Firefighter user
- FF IDs will be created in plug-in system and assign the role SAP_GRAC_SPM_FFID or its “Y” or “Z” equivalent to make it recognizable as FF ID
- FF Controller should also exist in the plug-in system with valid email ID as FF login notifications will be sent to controller’s email ID maintained in plug-in system
- FF log notifications are sent to FF controller’s mailed maintained in GRC system. Hence FF controller should exist in both GRC and plug-in systems
Access Request Configuration

Activate BC Sets (User Provisioning)

Add Connectors to Firefighting Scenario (PROV)

Maintain Configuration Settings

Maintain Provisioning Settings

Create Access Request

Complete Synchronization

Import Roles

Activate MSMP Workflow

Approve Access Request

Review Auto Provisioning
Step 1 – Activate BC Sets

- Activate BC Sets using SCPR20
  - GRAC_ACCESS_REQUEST_APPL_MAPPING
  - GRAC_ACCESS_REQUEST_EUP
  - GRAC_ACCESS_REQUEST_PRIORITY
  - GRAC_ACCESS_REQUEST_REQ_TYPE
Step 2 – Add Connectors

- Navigate to Tcode SPRO → SAP Reference IMG → expand Governance, Risk and Compliance → Common Component Settings → Integration Framework → Maintain Connection Settings
- Enter PROV in Integration Scenario and add the connector to the scenario
Step 3 – Maintain Configuration

- Maintain the provisioning details in SPRO IMG
Step 4 – Workflow Configuration

• Activate MSMP Workflow configuration and activate
Step 5 – Role Import

- Perform Role Import in the BC menu for Role Mass Maintenance
- Complete Step 1, 2, skip 3, and 4. Run the import.
Step 6 – Run Repository Sync Job

• Using Tcode GRAC_REP_OBJ_SYNC, initiate a repository sync job in background
Step 7 – Create Access Request

- Execute Transaction BC and within the My Home tab, click on Access Request to launch the Access Request screen
- Fill in description and request details
Step 7 – Create Access Request (cont.)

- Click User Details tab and fill in required information
- Click Roles Button and search and select appropriate roles for the user
- Submit the Request
Step 8 – Approve the Access Request

- Work Inbox, click the approval required
- Enter description and Submit to Approve Request
What We’ll Cover

• Technical Architecture
• Sizing
• Landscape and Client Strategy
• Implementation
• Upgrade and Migration Important Points
• Post-Installation and Configuration
• Job Processing
• Landscape Connectivity
• Performance
• Technical Tips
• Monitoring
• Wrap-up
Job Scheduling Hints

- Do not run all the jobs at the same time; space them out at least one hour apart
- Use variants to set up the jobs for FULL BATCH and INCREMENTAL BATCH. Make sure the connector name is specified. Schedule them in the background using SM36.
- In some cases, it is better to run a job for one connector at a time
- The factory calendar will have to be set up to schedule jobs on certain days
- It is best to run them in a certain order
- Offline/Online Risk Analysis is still a choice with the ARA Batch Risk Analysis job
- Filters are important for Batch Risk Analysis jobs
Access Control Jobs to Schedule

- **GRAC_ACTION_USAGE_SYNC** Daily Action Usage Job
- **GRAC_PFCG_AUTHORIZATION_SYNC** Weekly Profile Generator (PFCG) roles authorization synchronization
- **GRAC_ROLE_USAGE_SYNC** Daily Role usage synchronization
- **GRAC_ROLEREP_PROFILE_SYNC** Daily Role repository profile synchronization
- **GRAC_ROLEREP_ROLE_SYNC** Daily Role repository role synchronization
- **GRAC_ROLEREP_USER_SYNC** Daily Role repository user synchronization
- **GRAC_SPM_AUDIT_LOG_SYNC** Weekly Emergency Access Management (EAM) audit log synchronization
- **GRAC_SPM_LOG_SYNC_UPDATE** Weekly Emergency Access Management (EAM) log synchronization
- **GRAC_SPM_WORKFLOW_SYNC** Weekly Emergency Access Management (EAM) workflow synchronization
- **Batch Risk Analysis Job** Daily Risk Analysis Job
## Batch Jobs Table for ARA and SPM

<table>
<thead>
<tr>
<th>Job Name (ARA JOBS)</th>
<th>Job Type</th>
<th>Frequency</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRAC_REPOSITORY_OBJECT_SYNC</td>
<td>Full</td>
<td>Weekly</td>
<td>User/Role/Profile Sync; one time and then monthly (outside of core business hours) to make sure that everything is up-to-date</td>
</tr>
<tr>
<td>GRAC_BATCH_RISK_ANALYSIS</td>
<td>Full</td>
<td>Weekly</td>
<td>User/Role/Profile Batch Risk Analysis; one time and then monthly (outside of core business hours) to make sure that everything is up-to-date</td>
</tr>
<tr>
<td>GRAC_REPOSITORY_OBJECT_SYNC</td>
<td>Incremental</td>
<td>Daily</td>
<td>User/Role/Profile Sync</td>
</tr>
<tr>
<td>GRAC_BATCH_RISK_ANALYSIS</td>
<td>Incremental</td>
<td>Daily</td>
<td>User/Role/Profile Batch Risk Analysis</td>
</tr>
<tr>
<td>GRAC_PFCG_AUTHORIZATION_SYNC</td>
<td>–</td>
<td>Weekly</td>
<td>Authorization synchronization for (PFCG) role's authorization synchronization</td>
</tr>
<tr>
<td>GRAC_ACTION_USAGE_SYNC</td>
<td>–</td>
<td>Daily</td>
<td>Action Usage synchronization</td>
</tr>
<tr>
<td>GRAC_ROLE_USAGE_SYNC</td>
<td>–</td>
<td>Daily</td>
<td>Role Usage synchronization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Job Name (SPM JOBS)</th>
<th>Job Type</th>
<th>Frequency</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRAC_SPM_LOG_SYNC_UPDATE</td>
<td>Incremental</td>
<td>Hourly</td>
<td>Generates the EAM activity log</td>
</tr>
<tr>
<td>GRAC_SPM_WORKFLOW_SYNC</td>
<td>Full</td>
<td>Hourly</td>
<td>Compiles the EAM logs together by controller and triggers the log review workflow</td>
</tr>
<tr>
<td>GRAC_SPM_AUDIT_LOG_SYNC</td>
<td></td>
<td>Weekly</td>
<td>Emergency Access Management (EAM) audit log synchronization</td>
</tr>
</tbody>
</table>
Background Jobs for Process Control

- Workflow Jobs Scheduled with SWU3
  - GRFN_AM_JOBSTEP_MONITOR, hourly job, monitoring program to update job and job step status
  - /GRCPI/GRIA_AM_CHANGELOG (in plug-in system), daily job, captures the Change logs in the Plug-In system
  - Transfer Work Items to Replacement Job, transfers work items from users that are no longer working in the process control and risk management applications to the replacement users entered in the system for these users
  - GRFN_DATAMART_MAINTAIN, used for maintaining and uploading the data to data mart
  - Transfer Work Items to Replacement, run daily, program transfers work items from past users
  - Execute KRI Queries and Evaluate Business Rules, (Risk Management Job), run daily, Schedule the report GRRM_KRI_RUNTIME
  - Schedule Job for Sending Email, runs every 3 minutes, checks for new work items, determines email addresses of work item recipients
Scheduling the Action Usage Full Sync Job

- This job will take a long time to finish when the job is scheduled for the first time or when it has been a while since the last job was run
- Sometimes it may take up to a few hours to complete
- This job may be doing a full scan of table GRACACTUSAGE and get a large amount of data, which may take a very long time to complete
- The best practice for scheduling this job is, after the very first job is completed, immediately schedule a next period job that runs every 4 hours so that each job will select a much smaller amount of data and complete much quicker
Parallel Processing for Batch Risk Analysis Jobs

- The parallel processing option in batch risk analysis is to run the jobs with parallel processors, improve the performance, therefore reducing the total processing time.

- **STEP 1**
  - Check the number of background processes available for parallel processing, which is controlled by a system profile parameter: rdisp/wp_no_btc. This parameter determines the number of background processes configured in the system; these are used for many other tasks, including batch risk analysis. The number of background process depends on available system resources: CPU and Memory. The number of processes in batch risk analysis has to be less or equal to rdisp/wp_no_btc.

- **STEP 2**
  - Define “Max number of objects in a package for parallel processing” in IMG (SPRO transaction) as Governance, Risk, and Compliance → Access Control → Maintain Configuration Settings.
  - Set the following parameter.
    - **Param Group** | **Param ID** | **Parameter Value**
      - Risk Analysis | 1034 | 100
  - If this entry is missing, create a new entry. If the entry is available, update the parameter value. If the number of users/roles is very high, this parameter can be set as high as 500.
Parallel Processing for Batch Risk Analysis Jobs (cont.)

- STEP 3 → Configure “Maximum number of parallel processes in batch risk analysis” in IMG (SPRO) as follows: Governance, Risk, and Compliance → Access Control → Distribute Jobs for Parallel Processing
- If no record is available for application type GRAC_SOD, create a new entry as
  - Application Type – GRAC_SOD, Server Name – # Select the Server Name, Number of processes –
  - If you see a warning “Server-specific settings for job distribution are not transported,” just press enter key to continue
  - Number of processes has to be less than or equal to system profile parameter, rdisp/wp_no_btc
- Then, Save your changes
Parameters for Sync Jobs

- If you see that all of the above parameters are correctly sized and you still get same dump, please consider lowering values for the following parameters in transaction SPRO: click node Governance, Risk, and Compliance → Access Control → Maintain Configuration Settings.
  - Parameter Group = “Performance”
  - Parameter ID 1121 (Batch size for User sync)
  - Parameter ID 1122 (Batch size for Role sync)
  - Parameter ID 1123 (Batch size for Profile sync)

- Setting these parameters to lower level ensures that when GRC box makes a plugin call, then the number of objects to be synced in one call will be lower, and corresponding data can be handled by internal table.

- Note: Setting this parameter to lower level will make GRC box make more plugin calls than higher levels, as lower value for the parameters would mean that, in single plugin call, the number of objects to be synced should be lower.
Monitor the Batch Risk Analysis Jobs

- Batch Risk Analysis job scheduled in background
- Whenever batch risk analysis job scheduled, job triggers and can be processed in SM37. You can track the status of job in SM37.
- Use transaction “GRACRABATCH_MONITOR” or, in IMG, (SPRO Transaction) ➔ Governance, Risk, and Compliance ➔ Access Control ➔ Access Risk Analysis ➔ Batch Risk Analysis ➔ “Monitor Batch Risk Analysis”
- Search your job ➔ Select your job ➔ Double click to your job OR click on “Show Details” button
Tip — Best Practices for Improving Performance of EAM Log Sync Job

• The reason for the slow performance:
  ◦ The Log Sync Job is not Scheduled Hourly, so the Data is being synced for Long Time Intervals
  ◦ Large Number of Connectors are Configured for FFID Transactions
  ◦ The Number of FFIDs is Large for one Target Connector

• These are the Recommendation for Improving the Sync Job Performance
  ◦ The Log Sync Jobs should be Scheduled Hourly in SM36 as Background Job
  ◦ The Program used for Log Sync Job is “GRAC_SPM_LOG_SYNC_UPDATE”
  ◦ For Complex Landscapes, the Background Job should be Scheduled individually for each Target Connector; the sync Job takes Connector as an input parameter, and variant should be saved for each connector
  ◦ The Variants can be saved by executing the Program “GRAC_SPM_LOG_SYNC_UPDATE” in SE38. Provide the Input Parameters’ Connectors, press the Save button, and provide the Variant Name.
  ◦ When the Sync Job is Scheduled, the saved Variant should be mentioned for the Sync Job in SM36 as a Variant
Tip — Repository Object Sync Job Problem

- While running Repository Object Sync jobs, error occurs. “No more storage space available for extending an internal table” in SLG1. Check plug-in system in transaction ST22 and find dumps which mention the same error.
- The reason is that the system is not able to extend the internal table, as the data was too huge to be handled by internal table
- Set following parameters to correct levels as per sizing guidelines:
  - ztta/roll_area
  - ztta/roll_extension
  - abap/heap_area_total
  - abap/heap_area_dia
  - abap/heap_area_nondia
  - em/initial_size_MB
What We’ll Cover

- Technical Architecture
- Sizing
- Landscape and Client Strategy
- Implementation
- Upgrade and Migration Important Points
- Post-Installation and Configuration
- Job Processing
- Landscape Connectivity
- Performance
- Technical Tips
- Monitoring
- Wrap-up
**GRC Plug-In Tips**

- For SAP NetWeaver 7.30 support, use the GRCPINW 7.10 plug-in
- For SAP NetWeaver 7.31 and 7.40 support, use the GRCPINW 7.31 plug-in
- There is no need to install any Attribute Change Package (ACP) for these
- GRC Plug-in 10.0 can be used with GRC 10.1 systems and GRC plug-in 10.1 can be used with GRC 10.0 systems
- Backward Compatibility since Access Control 10.0 SP10 with newer plug-ins
  - The backward compatibility of GRCFND_A V1000 for Access Controls starts with Support Pack 10. Until SP10, both GRCFND_A and plug-in add-ons GRCPINW & GRCPIERP need to be one the same level.
  - However, from SP10 onwards, this is not required. This means that the add-on GRCFND_A on GRC system can be upgraded without the need to upgrade the plug-in add-on to the same level, provided the plug-in is at a minimum SP level of SP10.
  - In other words, once the plug-in is on SP10, the GRC add-on GRCFND_A can be upgraded to SP11 or higher without upgrading the plug-in
  - This backward compatibility also applies to the GRC 10.1 releases
GRC Plug-In Tips (cont.)

• Backward Compatibility for Process Control 10.0 and 10.1
  ◆ The backward compatibility of GRCFND_A V1000 for Process Controls has been introduced from support pack 12. Once the GRC system and GRC plug-ins are on SP12, it will no longer be mandatory to upgrade the plug-in in case the support pack in GRC system is upgraded to higher levels.

• Please note the following points before upgrade to the AC 10.1 plug-Ins
  ◆ Recommendation is to upgrade both front-end (GRCFND_A) and back-end plug-in (GRCPINW & GRCPieriP) components to AC 10.1, which also contains the AC 5.3 RTA
  ◆ During the time of transition, you can still connect to AC 10.1 plug-in (GRCPINW & GRCPieriP) from AC 10.0 front end.
  ◆ And also, you can connect to AC 10.0 Plug-in (GRCPINW & GRCPieriP) from AC 10.1 front end as long as support pack of AC 10.0 plug-in is SP10 and above. However, some new AC 10.1 functionalities, such as Organization Rule Wizard, Custom User group creation, and EAM DB log collection, will not work.
GRC 10.0/10.1 Plug-In Details for Co-Existence with AC 5.3

- SAP Note 1590030: GRC10 plug-in and 5.3 VIRSA plug-in (RTA) co-existence, Access Control 5.3 can be used simultaneously with AC 10.1 plug-in systems while in the process of completing migration/upgrade
  - Meant to be temp solution while completing migration/upgrade
- Minimum requirements are GRCPINW SP04 (equivalent to AC 5.3 VIRSANH SP16 and VIRSAHR SP14) and AC 5.3 Java
- Current version is GRCPINW SP (SP12) and AC 5.3 Java SP23
- Anything after AC 5.3 Java SP18 must check with GRC Support to see if there are any compatibility issues between the later AC Java SPs and the GRC 10.1 support packages
GRC 10.0/10.1 Plug-In Details for Co-Existence with AC 5.3 (cont.)

- New GRCPINW 7.31 Plug-in SP02 is equivalent to SP11
- Strategy
  - Major fixes to 5.3 will be included in the 10.0/10.1 support packages for up to one year from v10 GA (General Availability)
  - Minor issues will have an SAP Note released, if possible
System Connector Tips

• System Connectors are assigned to a Connector Group and, later, Connector groups are classified as cross-system type to get the cross-system Risk Analysis

• Wrong configuration will result in inconsistencies in the User data in the GRC Access Control Repository; may assign User to a different Connector

• After assigning the Connector groups to cross-system, Full Synchronization or Incremental Synchronization may resolve the problem

• If not, clean-up/truncation of data from the GRC Access Control Repository tables is necessary. Then, re-start from the beginning of the configuration (this is needed if changing connectors to different system in a sandbox or development system).
Step 1: Connector Setup — RFC Connections

- First, set up RFC Connections to the Plug-In systems, such as the ERP system (the name of the connector will be critical)
Step 2: Connector Setup — Logical Groups

- Each rule set is activated and linked into a separate logical group (technical name in brackets):
  - GRAC_RA_RULESET_SAP_R3: Rules for ERP including Basis and HR (SAP_R3_LG)
  - GRAC_RA_RULESET_SAP_HR: Rules for HR only (SAP_HR_LG)
  - GRAC_RA_RULESET_SAP_NHR: Rules for ERP excluding HR and Basis (SAP_NHR_LG)
  - GRAC_RA_RULESET_SAP_BASIS: Rules for Basis (SAP_BAS_LG)
  - GRAC_RA_RULESET_SAP_APO: Rules for APO (SAP_APO_LG)
  - GRAC_RA_RULESET_SAP_CRM: Rules for CRM (SAP_CRM_LG)
  - GRAC_RA_RULESET_SAP_ECCS: Rules for ECCS (SAP_ECC_LG)
  - GRAC_RA_RULESET_SAP_SR: Rules for SRM (SAP_SR_LG)
  - GRAC_RA_RULESET_JDE: Rules for JD Edwards (JDE_LG)
  - GRAC_RA_RULESET_ORACLE: Rules for Oracle Apps (ORACLE_LG)
  - GRAC_RA_RULESET_PSOFT: Rules for PeopleSoft HRMS (PSOFT_LG)
Step 3: Connector Setup — Connector Assignments and Connector Group

- Next, set up Connector Assignments and Connector Groups
- The Connector Group is important for the Rule Set activated (from Step 2)
Step 4: Connector Setup — Maintain Connector Settings by Integration Area

- Set up the Connector Assignment for each of the Integration Scenarios
- Note: Must perform all scenarios’ setup regardless of using or not
Step 5: Connector Setup — Maintain Connector

- Simple Setting to Map the Target Connector to the Application Type
Step 6: Connector Setup — Assign Connector Groups to Actions and Target Connectors

- Assign the Connector Group, the Actions, and the Target Connectors
- Usually Assign all Actions, set default
What We’ll Cover

• Technical Architecture
• Sizing
• Landscape and Client Strategy
• Implementation
• Upgrade and Migration Important Points
• Post-Installation and Configuration
• Job Processing
• Landscape Connectivity
• Performance
• Technical Tips
• Monitoring
• Wrap-up
Performance Topics in This Section

- GRC System performs analytics processing. This requires special considerations for performance.
- Rules Discussion – Performance of Access Control depends heavily on the Rule Set being set up correctly. This is important.
- Risk Analysis Considerations
- Risk Analysis Storage Considerations
- Clean up of Data
- Jobs and Parallel Processing of Analysis Jobs (this is in the Job Processing Section of this presentation)
Risk Analysis Rule Set
First Step – Getting the Rule Set Correct

- Access Risk Management (ARA) comes delivered with SAP’s best practice, standard-delivered Rule Set (used as a starting point for new implementations). The Rule Set is delivered in BCSETS and loaded using transaction SCPR20.

- For those who already have implemented Risk Analysis and Remediation (RAR) (such as previous version 5.3), you should have a customized Rule Set to meet the business requirements. Rather than activate the new Rule Set delivered by SAP in the BCSETS in GRC 10, it is best to consider importing the customized Rule Set into GRC 10 using the SPRO Rule Set import function.

- It is a good idea to evaluate the changes incorporated into the most recent SAP Rule Set to determine if the changes should be added to the custom Rule Set. Any modifications desired can be manually made using the Rule Architect feature of access risk management.

- Administrators may decide it is easier to implement this new rule set (which will overwrite existing custom Rule Set) and just make the customization changes again to the newly imported default Rule Set. This works best when minimal changes to the default Rule Set have been made.

- See SAP Note 986996 for an explanation of the Rule Set (has an attachment to the note)
Risk Analysis Rule Set
Second Step – Using the Standard-Delivered Rule Set

• The set of rules that SAP provides hit the majority of global requirements for the basic processes: Finance, Procure to Pay, Order to Cash, etc.
• Special rules have been provided for other specialty areas by working with partners and customers for SAP CRM, HR, and ECC, etc.
• The whole purpose is to provide a solid starter set rather than building rules from scratch. The delivered Rule Set is meant to cover the major risk areas present for the majority of customers.
• Not every SAP application is included in the delivered Rule Set and, at this point, there are no plans to further develop additional industry-specific components or add-on product rules.
• The time the company spends is to make sure the risks are appropriate for their implementation of SAP and adding custom-related transactions, rather than starting from scratch.
• SAP does deliver a BASE Rule Set for customers to use. However, please review SAP Note 986996 for more information. It is up to each customer to customize their rules to address their specific control requirements.
Risk Analysis Rule Set
Third Step – Keeping the Rule Set Updated

• A new Rule Set was delivered Q4 of 2014
• See SAP Note 2109459 – GRC Access Control – Access Risk Management Rule Update Q4, 2014
• GRC 10.1 SP10, GRC 10.0 SP20 includes the latest Rule Set included in the delivered BC_SETS (Access Control 5.3 Support Pack 23 includes the latest Rule Set)
• The note has an attached zip file called “2014_Q4_Rule_Update_Document.zip.”
• The attachment summarizes all of the delta changes made to SAP’s Rule Set for Q4 2014.
• Q4, 2014 Rule Set changes have been made in the below 3 BCSETS:
  ◦ GRAC_RA_Rule Set_SAP_BASIS BC Set
  ◦ GRAC_RA_Rule Set_SAP_R3 BC Set
  ◦ GRAC_RA_Rule Set_SAP_NHR BC Set
Steps for Risk Analysis

• STEP 1 → The first area to focus on is ensuring master data is complete and correct. Master data includes the following:
  - Risk Analysis and Remediation Rules
  - Critical Roles and Profiles
  - Configuration

• STEP 2 → Make sure the Rule Set is complete (mentioned in the previous discussion)
  - The GRC Access Control components rely on the Rules to identify and report on segregation of duties risks
  - If these Rules are incomplete or incorrect, the risks will not be accurately reported

• STEP 3 → Verify the Connectors are set up properly for the systems being analyzed
Steps for Risk Analysis (cont.)

- STEP 4 ➔ Generate the Rules in SPRO under Access Control, Access Risk Analysis
- STEP 5 ➔ Maintain Exclude Objects for Batch Risk Analysis
  - By default, the application performs batch risk analysis on all objects in the specified system
  - Choose to exclude specific objects that you know are safe or do not need to be analyzed. Very important step for performance reasons.
- STEP 6 ➔ Set up Parallel Job Processing for the Batch Risk Analysis Jobs
- STEP 7 ➔ Run the User/Role/Profile Sync and Auth. Sync Jobs
- STEP 8 ➔ Run the Batch Risk Analysis Job, Monitor the Job, Test the Results
Batch Risk Analysis Impacts

- Schedule the risk analysis job for selected users/roles/profiles and for selected systems
- Keeps snapshot of every user/role/profile violation in the database for management reporting and analysis
- There may be a large database growth for first-time run. After that, there will be less database growth, since it will analyze only the incremental objects.
- The initial large database growth depends on the rule set, number of authorizations, and number of violations per user/role/profile
  - This may be large if users/roles were never cleaned up
- For certain cases, you may able to switch off the batch risk analysis results being stored in the database by setting configuration parameter 1027 (Enable offline Risk Analysis) to “No”
  - This will drastically reduce the database growth from batch risk analysis, but will still update the management dashboard data
- Please note that this option is not viable if you desire to use offline analysis instead of real-time ad hoc analysis, if using the report SOD Review, or if enabling BW reporting
Ad Hoc Risk Analysis Impacts

- Ad hoc Risk Analysis is run by users who are executing risk analysis in real-time in either foreground or background.
- These results are stored either in database or file locations, depending on the settings in configuration in the IMG.
- The default is the database option, but you can change it to file and provide the shared file location to store these results.
- There are pros and cons for both options.
- The growth of database or file system from ad hoc analysis also depends on the same factors for batch risk analysis, but, in addition, more space is consumed when ad hoc analysis is executed frequently on the same roles (space is repeated).
- Database or file system growth can be an issue.
  - Clean up is possible for these tables and files.
Remediating Risks Helps the System

• At first, administrators may be overwhelmed with the amount of risks identified
• The high number of risks that are identified directly correlate to the performance of all GRC Access Control components
• The more risks that exist in the system, the longer reporting and analysis will take
  • Administrators must understand how to remediate the risks at the role and user level
• Remediation means that either the risk is removed or the risk is mitigated so that the segregation of duties concern is properly addressed
  • Focus on remediation, so that the risks are truly controlled
• Performance issues may occur in the system due to large number of risk violations
Critical Roles

- In every system, there will be roles and profiles that inherently have mass numbers of conflicts. These are the roles that are normally given to system user IDs (like those used to run jobs) or to Firefighter IDs.
- These types of roles should be controlled outside of identifying the individual risks inherent in the roles. Instead, the roles and profiles should be added to the Critical Roles and Profiles master data tables and the assignment of these roles reviewed on a periodic basis.
- To add roles to these tables, go to Rule Architect – Critical Roles/Critical Profiles. The data is system-dependent, so critical roles and profiles should be loaded for all connected systems.
- Once done, go to Configuration – Risk Analysis – Additional Options and ensure the option Ignore Critical Roles & Profiles is set to Yes
- This will ensure that when these critical roles are assigned, the risks are NOT shown on the report. Again, these roles should be controlled at the assignment level, not at the individual risk level.
Types of Risk Analysis — Action vs. Permission

- Main differences between running Action level vs. Permission level Risk Analysis
  - Action level only compares at the transaction level
  - Permission level further filters the results based on the authorization objects set up in the rules
  - Running at permission level is just to further filter the conflicts based on any authorization object setting you have in the rules. If there are no authorization objects enabled in the rules, the same action risk will show at permission level.
  - There will never be any conflict that will have a permission level risk but not a corresponding action level risk. There are risks that will show at action level, but not at permission level, because the user doesn’t have all the required authorization objects.
Review of Recommendations for Batch Risk Analysis

- Do not select action level analysis when permission level analysis is selected. It will reduce database growth from batch risk analysis, as action violations-related tables will not be populated.
- To reduce the large number of violations from SAP_ALL or SAP_NEW like profiles define these profiles as critical profiles and configure parameter 1031 (Ignore critical roles/profiles analysis) to ignore the violations that are coming due to these critical roles/profiles.
- For certain cases, you may be able to switch off the batch risk analysis results being stored in the database by setting configuration parameter 1027 (Enable offline Risk Analysis) to “No.” This will drastically reduce database growth from batch risk analysis and update only management dashboard data.
- Full vs. Incremental Analysis: When a new system is added to the GRC system or run for the first time, please run batch risk analysis in FULL analysis mode. For any subsequent run do it in incremental mode which will reduce total processing time drastically and may reduce database growth. Based on business requirements, a subsequent FULL analysis mode run can be performed, if needed.
New — Downloading Access Risk Data

- A new utility has been created which will allow you to download Risk Analysis data in text form which can be opened using MS Excel
- This may be useful if the amount of risk data is huge and must be stored outside of the database
- The utility is called GRAC_EXPORT_REPORT_SPOOL
- The utility is provided in SAP Note 1792254 – Export of Risk Analysis reports may time out
- Implement SAP Notes 1708317 and 1748189 before implementing this note
- Note: The file is stored on the application server and may need to be transferred to a shared drive
File System vs. Database Storage for Risk Analysis

- Using file-based storage may be preferred and recommend during initial loads, testing periods, or sometimes, even for production
- Using the File system is relatively faster in performance (time to complete the risk analysis job)
- The disadvantage is the data must be backed up and restored using operating system tools separate from the database
- The advantage to using the Database is the back-up and restore jobs using database tools are done by default and consistency is ensured
- The disadvantage is the database is slower than file system storage, increases the load in the database, and requires maintenance work for DBA if database grows faster
- Settings for these options are configured in the IMG (using SPRO) in Maintain Configuration Settings. Param ID 1053, Value “D” or “F” and Param ID 1052 for Location of the Files if “F” is used (Database is default).
Clean Up — Deleting the Rule Set

- Steps to clean out the rule set and all data (for major clean up):
  - NOTE: Not for Production System, only Sandbox and Development Systems
    - GRAC_DELETE_ACCESS_RULES ➔ This report will delete rules for related table’s data, synchronization table’s data, and violation table’s data. The execution of this report will be based on the selection of connector. After execution of report, log will be maintained in SLG1 with “GRFN” as object and “AC_REP” as subobject. This log will display the user name of the person who has executed the report and the connector name used during execution of report. This one is the same as SPRO ➔ SOD Rules ➔ Delete SOD Rules in the system.

- GRAC_DELETE_ACCESS_RULES_ALL ➔ This report will delete access rules for related table’s data, Synchronization table’s data, and violation table’s data, but not based on the connector. It will delete all connector table data that exists in the system. You can check the log in SLG1 with “GRFN” as object and “AC_REP” as subobject (Not on a menu).
- Also delete the Functions, Access Risks, and Rule Set from the Rule set-up menu. Rule Set name is last to be deleted.
Clean Up — Manually Deleting the SOD Table Data (Worst Case)

- List of tables in batch risk analysis:
  gracuseractvl, gracuseractvlext, gracusercrpvl, gracuserprmvl, gracuserprmvlxt, gracusermgmtsum, 
gracusermgvcnt, gracroleactvl, gracroleactvlext, gracrolecrpvl, gracroleprmvl, gracroleprmvlxt, 
gracrolegmtsum, gracrolemgvcnt, gracprofactvl, gracprofactvlext, gracprofcrpvl, gracprofprmvl, gracprofprmvlxt, 
gracprofmgmtsum, gracprofmgvcnt, gracmgriskd, gracmgrulecnt

- Steps to clean up the tables:
  1. GoTo SE14 transaction
  2. Choose table option and enter <TABLENAME>
  3. Click on Edit button
  4. Choose processing type background
  5. Click on delete database table button
  6. Once the job is completed, then click on create database table

- Once the tables are cleaned up, reorganize the database
- Following the above steps, you can clean up the database, reduce growth of database, and manage storage for risk analysis
What We’ll Cover

• Technical Architecture
• Sizing
• Landscape and Client Strategy
• Implementation
• Upgrade and Migration Important Points
• Post-Installation and Configuration
• Job Processing
• Landscape Connectivity
• Performance
• Technical Tips
• Monitoring
• Wrap-up
Sizing Consideration — Table Growth for Ad Hoc Risk Analysis

- Online ad hoc risk analysis stores the risk analysis results in temporary tables before rendering to users.
- The result of the risk analysis is stored in the following tables:
  - GRACSODREPDATA
  - GRACSODREPINDEX
  - GRACSODREPSTATUS
- Every time ad hoc risk analysis is performed, the result of the analysis is appended in these tables and, as a result, there is a growth in the database.
- The growth in the table depends on the number of users/roles analyzed and the number of violations that they have.
- In some cases, it has been seen that the size of the table was increased by 10 GB while executing ad hoc risk analysis.
Tip — Clearing Space in Tables for Ad Hoc Risk Analysis

- Data in the ad hoc Risk Analysis tables can be cleared by running the report GRAC_DELETE_REPORT_SPOOL
- Schedule as a daily job or run manually anytime
- The report will clear the data from the below temporary tables:
  - GRACSODREPDATA
  - GRACSODREPINDEX
  - GRACSODREPSTATUS
- This report will delete the data from the table space or the file system, whichever you use as storage type
- Refer to SAP Note 1580877 → Best practices in storage management for SoD analysis jobs
**Tip — Significant Database Tables and Growth for Batch Risk Analysis Jobs**

<table>
<thead>
<tr>
<th>Batch Risk Analysis Tables – Users</th>
<th>Roles</th>
<th>Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>gracuseractvl</td>
<td>gracroleactvl</td>
<td>gracprofileactvl</td>
</tr>
<tr>
<td>gracuseractvlext</td>
<td>gracroleactvlext</td>
<td>gracprofactvlext</td>
</tr>
<tr>
<td>gracusercrpvl</td>
<td>gracrolecrpvl</td>
<td>gracprofilecrpvl</td>
</tr>
<tr>
<td>gracuserprmvl</td>
<td>gracroleprmvl</td>
<td>gracprofileprmvl</td>
</tr>
<tr>
<td>gracuserprmvlext</td>
<td>gracroleprmvlext</td>
<td>gracprofprmvlext</td>
</tr>
<tr>
<td>gracusermgmtsum</td>
<td>gracrolemgmtsum</td>
<td>gracprofmgmtsum</td>
</tr>
<tr>
<td>gracusermgvcound</td>
<td>gracrolemgvcound</td>
<td>gracprofmgvcound</td>
</tr>
<tr>
<td><strong>HR Objects:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gracrobjectactvl</td>
<td>gracmgriskd</td>
<td></td>
</tr>
<tr>
<td>gracrobjectcrpvl</td>
<td>gracmgrulecount</td>
<td></td>
</tr>
<tr>
<td>gracrobjectprmvl</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

** This table can grow significantly (60GB in some cases) **
Common Problems — Workflow Setup Incomplete

- The Workflow Administration tools are on the SPRO Workflow menu
- Set up the customizing so all workflow items are green
Common Problems — Workflow Setup

- Make sure the Tasks are set up correctly. General tasks must be set up for the TS tasks.
- Make sure the settings are correct for the WS objects, that they are activated, and that linkage is set correctly.
Technical Tips — Application Logs

- Application Logs
  - The application logs can be monitored with transaction SLG1
  - The Access Control log object is GRAC
  - The Process Control log object is GRPC
  - The Risk Management log object is GRRM
  - The shared components (for Process Control and Risk Management) log object is GRFN
Technical Tips — SMICM/HTTP Set-Up Points

- GRC suite 10.1 is based on ABAP Web Dynpro technology; therefore, it includes pure Web-based applications
- Set up Web services in the ABAP stack using SMICM
  - Set up HTTP server ports
  - Create profile parameters in RZ10
- Set time-out values high enough for users not to experience session terminations
  - Example below allows for one hour

```
.icm/server_port_0 | PROT=HTTP,PORT=80$$,TIMEOUT=3600,PROC_TIMEOUT=1800
```

<table>
<thead>
<tr>
<th>No.</th>
<th>Log</th>
<th>Service Name/Port</th>
<th>Host Name</th>
<th>Keep Alive</th>
<th>Proc.Time</th>
<th>Actv</th>
<th>External Bind</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HTTP</td>
<td>8000</td>
<td>socwester37_solution</td>
<td>3.000</td>
<td>1.800</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>HTTPS</td>
<td>8200</td>
<td>socwester37_solution</td>
<td>3.000</td>
<td>1.800</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>SMTP</td>
<td>0</td>
<td>socwester37_solution</td>
<td>30</td>
<td>00</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>
Technical Tips — Memory Settings forRunning Batch Risk Analysis

• Profile parameters enable you to set up your memory management system to get maximum benefit from it. By setting the parameters correctly, you can adjust memory management exactly to your resources and requirements.

• A few profile parameter tuning requirements for SOD analysis are shown below. It is recommended to review all profile parameters of memory management.

• Memory parameters can be adjusted to run SOD analysis based on available resources and requirements

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>abap/heap_area_dia</td>
<td>40000000000</td>
</tr>
<tr>
<td>abap/heap_area_nondia</td>
<td>60000000000</td>
</tr>
<tr>
<td>abap/heap_area_total</td>
<td>100000000000</td>
</tr>
<tr>
<td>em/initial_size_MB</td>
<td>9000</td>
</tr>
<tr>
<td>abap/buffersize</td>
<td>3000000</td>
</tr>
</tbody>
</table>
Technical Tips — Process Control Performance

- Increase reporting performance by creating the reporting data mart buffers for each timeframe
  - Schedule the Data Mart background job to fill the Data Mart tables with timeframe-based data (ALL/SPRO)
- Set up and create buffers for dashboards based on timeframes
  - The dashboard feature uses buffers to increase performance when loading data for reports (PC/SPRO)
- Enhance system performance for calling up reports by creating an index for the table Infotype 1001 DB Table (HRP1001) (PC/SPRO)
- Activate Shared Objects Memory to improve performance
  - Shared Objects Memory improves response for certain data, such as organizational hierarchy, account group hierarchy, and catalogs
Technical Tips — Settings for SHMM

• Transaction SHMM provides an overview of the area instances in the shared objects memory of the current application server
• Settings for the Shared Area should be set in RZ10 Profiles
Technical Tips — Settings for Communications

- Single Sign-On (SSO): Must be set up for Portal → ABAP, and all systems must appear in same DNS domain
- Secure Sockets Layer (SSL): If configured, SSL requires certificates to be signed by CA for BC. Then, HTTPS is needed during login for password only.
- SMTP: Email integration for notifications pointing to the company’s SMTP email gateway; use transaction SCOT
- Email: Inbound gateway for surveys and forms may be configured
- Portal and ABAP: Must both be either HTTP or HTTPs setup, but not mixed
- Timeouts for SMICM in ABAP: Set up values for 1 hour or 3,600 seconds
- Solution Monitoring: Basic monitoring should be considered for all GRC applications
Technical Tips — Crystal Reports

• The setting is in the Windows IE Browser. Change the following settings in your browser as follows:
  • Go to TOOLS → INTERNET OPTIONS
  • Go to Security → Local Intranet Custom Level
  • Set Display mixed content to DISABLE
  • I also added both URLs to my trusted sites with and without the https/http
Technical Tips — Adobe Document Services Requirements

- An instance of Adobe Document Services (ADS) should be accessible from the GRC AS ABAP for generating offline forms (e.g., for PC and RM)
- Although it is technically optional, it is highly recommended for generating PDF reports
- Adobe Document Services is recommend for offline RM surveys
- This ADS can be an existing instance and can also be shared with other applications
- The Portal’s AS Java can contain an Adobe Document Services instance, so Portal and ADS may be shared on one AS Java instance
- It runs with both 7.02, 7.31, and 7.40 Java Systems
Technical Tips — Document Search Engine (TREX)

- TREX may be used for searching documents attached to objects in some GRC solutions, such as Process Control or Risk Management
- Install TREX (enterprise is not needed)
- Connect the RFC using the Administration tool (shown below)
Technical Tip — SAP BW Integration for Advanced Custom Reporting

- SAP Business Warehouse integration
  - SAP BW can be used for reporting via the GRC BI Content
  - Two parts needed:
    - SAP BW 7.40 is part of the ABAP stack
    - GRC BI Content is part of BI Content 7.47 (10.1 is supported by this version of BI Content)
  - SAP Notes and supplement guides available to help integrate BW content with the GRC solutions
- PC/RM 10.1 will work with the delivered PC/RM 3.0 BW content
  - SAP Note 1312030 – BI Content FAQ for GRC PC 3.0 and GRC RM 3.0, Supplemental guide is attached
  - SAP Note 1551203 – PC/RM BI Datasources, PC/RM 10.0 BI extractors can be used with GRC PC/RM 3.0 BI content
- SAP HANA is the new preferred method of reporting
Technical Tip — Web Services

- Used to integrate with non-SAP systems
- Used to integrate with Identity Management solutions
- Use transaction SOAMANAGER to configure the web services
- Web services can be tested using a Java stack in the landscape
Technical Tip — MSMP and BRF+ Workflow

- Old workflow in GRC AC 5.3 CUP application, such as Initiator, Stage, and Path, is replaced with MSMP and BRF+ Workflows
- Multi-Stage Multi-Path (MSMP) process workflows used in 10.1 Access Control
  - Maintain these workflows using MSMP configuration in SPRO. Maintain Rules, agents, variables/templates, paths, and routes
- Workflows are extended using function modules (ABAP skills may be needed)
- Ready-to-use MSMP workflow components are delivered by SAP under BC Set GRC_MSMP_CONFIGURATION
- Business Rule Framework plus (BRFplus) is a business rules system released with SAP NetWeaver 7.02 (EHP2) and 7.31/7.40 versions
- BRFplus workbench is a User Interface (UI) that enables users to define, test, and maintain rules for various business scenarios without needing ABAP code
  - Rules can be created for initiators, agents, and also for routing workflows on specific conditions
- Workflow configuration is in SPRO
Technical Tip — Content Lifecycle Management

- Content Lifecycle Management (CLM) is installed by the add-on POASBC component in ABAP stack
- CLM has the same (version) requirements as the GRC 10.1 suite and is installed during the GRC installation (CLM can be disabled if not required)
- CLM aims to support the management of application content
  - This is achieved by providing users with a consistent way to package, version-control, inspect, and import vendor content into their systems
  - It focuses on the capability to deliver content from vendors’ landscapes to customers’ landscapes
- CLM contains functions for transporting GRC business data (e.g., AC Rules or PC Controls)
SAP HANA Analytics Foundation for SAP Solutions for GRC

- HANA Analytics used for Access Risks:
  - This virtual data model provides the (building blocks) prerequisites for creating ad hoc reports for analyzing the access risks, access risk violations, incidents of SoD risk and mitigating control risk violations, org rules, mitigating controls, actions, functions, critical actions/roles/profiles, action usage, incidents, Segregation of Duties (SoD), and user access risk. Analysis areas include risks library, rules library, users, and roles.

- Based on this virtual data model, you can generate reports to answer the following business questions:
  - What are the access risk violations over the past six months?
  - What are the risk violations for a specific role?
  - What mitigating activities have been performed over the past three months?
  - What unmitigated risks exist in the system?
  - What is the history for SoD reviews?
  - What is the history for user access reviews?
<table>
<thead>
<tr>
<th>Transaction Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NWBC</td>
<td>Access the majority of the Access Control capabilities and reports (role: SAP_GRC_NWBC)</td>
</tr>
<tr>
<td>GRAC_ALERT_GENERATE</td>
<td>Alert generation</td>
</tr>
<tr>
<td>GRAC_BATCH_RA</td>
<td>Risk analysis in batch mode</td>
</tr>
<tr>
<td>GRAC_SPM and GRAC_EAM</td>
<td>Emergency Access Management (EAM)</td>
</tr>
<tr>
<td>GRAC_SPM_CLEANUP</td>
<td>Clean up SPM application data</td>
</tr>
<tr>
<td>GRACRABATCH_MONITOR</td>
<td>Batch risk analysis monitor</td>
</tr>
</tbody>
</table>
SAP GRC Lifecycle for GRC 10.1 Suite

- SAP NetWeaver 7.40 to 12/31/2020
- GRC 10.1 Target Release to customer date: 14 June 2013
- GRC 10.1 Target Ramp-Up Completion date: 31 January 2014
- GRC 10.0 unrestricted availability since 7/29/2011
- Maintenance information below current as of 3/1/2016

<table>
<thead>
<tr>
<th>Product/Version</th>
<th>Mainstream Maintenance End</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Process Control 10.0/10.1</td>
<td>12/31/2020</td>
</tr>
<tr>
<td>SAP Process Control 3.0</td>
<td>05/31/2013</td>
</tr>
<tr>
<td>SAP Risk Management 10.0/10.1</td>
<td>12/31/2020</td>
</tr>
<tr>
<td>SAP Risk Management 3.0</td>
<td>05/31/2013</td>
</tr>
<tr>
<td>SAP Access Control 10.0/10.1</td>
<td>12/31/2020</td>
</tr>
<tr>
<td>SAP Access Control 5.3</td>
<td>12/31/2015</td>
</tr>
</tbody>
</table>

* Requires login credentials to the SAP Service Marketplace

Source: http://service.sap.com/pam *
Current Software Support Package Levels

- Current as of 3/1/2015
- Recommended to install the latest Support Packages (SP)
- Installing GRC PI can be an issue if the SAP ERP system does not meet minimum SP levels
  - Check this early in the project!

<table>
<thead>
<tr>
<th>PACKAGE</th>
<th>COMPONENT</th>
<th>SUPPORT PACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP GRC AC/PC/RM 10.1</td>
<td>GRCFNDA_1100</td>
<td>SP12</td>
</tr>
<tr>
<td></td>
<td>GRCPINW V1100_700</td>
<td>SP12</td>
</tr>
<tr>
<td></td>
<td>GRCPINW V1100_731</td>
<td>SP13</td>
</tr>
<tr>
<td></td>
<td>GRCPINW_V1100_731</td>
<td>SP13</td>
</tr>
<tr>
<td></td>
<td>Portal Component 10.0 (7.30+)</td>
<td>SP10</td>
</tr>
<tr>
<td></td>
<td>Portal PI 10.0 (7.30+)</td>
<td>SP03</td>
</tr>
</tbody>
</table>
What We’ll Cover

• Technical Architecture
• Sizing
• Landscape and Client Strategy
• Implementation
• Upgrade and Migration Important Points
• Post-Installation and Configuration
• Job Processing
• Landscape Connectivity
• Performance
• Technical Tips
  • Monitoring
• Wrap-up
Monitoring – Topics

• Using Solution Manager and CCMS
• Monitor the following in the SAP Standard CCMS tool for process control, risk management, and access control applications:
  • Background job
  • Performance Overview
  • DB access time
  • System log
  • System errors
  • Web Services Call
  • Background Jobs
• Monitor the background job status for jobs that are aborted, canceled, or have been running for a long time
Monitoring – Workflow Jobs

- Set up workflow jobs using SWU3
Monitoring – Transaction SWI1: Work Item List

- If a workflow has been correctly triggered and started, at least one work item should be created. You can view the work items here. By default, all the work items of the last hour will be displayed.
Monitoring – Transaction SWIA: Process Work Item as Administrator

- You can use this report to execute work items for which you are not a possible agent.
- Using this work item selection, you can select the necessary work items and then execute them, complete them, or make them available again to the recipients.
Monitoring – Transaction SWPR: Workflow Restart After Error

This report can be used to display a list of workflows with errors for a particular selection period and then restart them. The benefit of this report is that it allows you to perform a mass restart of workflows.
Monitoring – Workflow Event Queue

- Doesn’t need to be enabled unless a huge quantity of workflows cause dialog processing overload
- Refer to SPRO – PC IMG
Monitoring – Email

- Check Transaction SCOT for errors
• Scheduler logs are only relevant for the Process Control application. To view the scheduler logs, log on to the portal, select a regulation workset, and click Evaluation Setup Monitoring Scheduler.
What We’ll Cover

• Technical Architecture
• Sizing
• Landscape and Client Strategy
• Implementation
• Upgrade and Migration Important Points
• Post-Installation and Configuration
• Job Processing
• Landscape Connectivity
• Performance
• Technical Tips
• Monitoring
• Wrap-up
Where to Find More Information

- Main GRC documentation available
  - Service/Support Marketplace (guides, software downloads, and SAP Notes) → http://support.sap.com
  - GRC Community on SCN → http://scn.sap.com/community/grc
- Documentation is now mostly centered at the SAP AC http://help.sap.com/grc-ac and SAP PC http://help.sap.com/pc websites, including the GRC products where links are provided to all documentation, including Master, Installation, Upgrade, Configuration, and Security Guides
- HANA Analytics for GRC (SAP HANA Live) → http://help.sap.com/hba
- GRC 10.1 system IMG information is key (Configuration Guide is not provided externally)
SAP GRC 10.1 – Good Installation Notes

- Read the following SAP Notes before starting your installation!

<table>
<thead>
<tr>
<th>SAP Note</th>
<th>Description – GRC 10.0/10.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1855332</td>
<td>Release strategy for SAP Access Control 10.1</td>
</tr>
<tr>
<td>1855403</td>
<td>GRCFND_A V1100 Installation and Upgrade</td>
</tr>
<tr>
<td>1855404</td>
<td>GRCPINW V1100 Installation and Upgrade</td>
</tr>
<tr>
<td>1855405</td>
<td>GRCPIERP V1100 Installation and Upgrade</td>
</tr>
<tr>
<td>1510002</td>
<td>Installing SAP GRC Portal 10.0, Information about installing the GRC_POR 1000 software component</td>
</tr>
<tr>
<td>1844875</td>
<td>Release restrictions for GRC Process Control 10.1</td>
</tr>
<tr>
<td>1855568</td>
<td>Install/Upgrade RTA for GRC Process Control 10.1</td>
</tr>
<tr>
<td>1855639</td>
<td>Upgrading SAP NW with GRC 10.1 Plugin for Process Control</td>
</tr>
<tr>
<td>1597627</td>
<td>SAP HANA connection</td>
</tr>
</tbody>
</table>
# SAP GRC 10.0/10.1 – Good Installation Notes

<table>
<thead>
<tr>
<th>SAP Note</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GRC Suite 10 – CRYSTAL REPORT ADAPTER:</strong></td>
<td></td>
</tr>
<tr>
<td>1353044</td>
<td>Installation Guide, Crystal Report Adapter</td>
</tr>
<tr>
<td>1366785</td>
<td>Crystal Reports ALV, Integration, Functional Restrictions</td>
</tr>
<tr>
<td>1362730</td>
<td>Crystal Reports ALV, Integration, Troubleshooting</td>
</tr>
</tbody>
</table>

| **GRC Suite 10 – OTHER IMPORTANT NOTES:**                                                   |
| 1514346    | BRF+ Various Bug Fixes in EHP2 (SP04-SP06)                                                      |
| 1519164    | Create BRF+ application name & ID for Continuous Monitoring                                  |
| 1533832    | AC 10.0: Changes to doc. by functional corrections in SPs AC 10.0                            |
| 1536525    | GRC Access/Process Control Upgrade Add-on Handling; this note provides information about upgrading |
| 1470670    | User-defined Fields for RM                                                                    |
| 1662113    | Using Access Control 5.3 with your 10.0 plug in systems                                       |
| 1590030    | GRC10 Plug-in & 5.3 VIRSA Plug-in (RTA) Co-Existence                                           |
| 1352498    | Support Pack Numbering – GRC Access Control                                                  |

| **BW SAP Notes**                                                                                 |
| 1312030    | BI Content FAQ for GRC PC 3.0 and GRC RM 3.0; supplemental guide attached to note             |
| 1667517    | GRC AC 10 Integration with BI                                                                 |
| 1551203    | PC/RM BI Datasources, PC/RM 10.0 BI extractors can be used with GRC PC/RM 3.0 BI content    |
7 Key Points to Take Home

- GRC solutions are based on SAP NetWeaver 7.40 and the ABAP system which provide a powerful and rich application platform
- Acquiring a complete understanding of the architecture for each GRC solution and the required components and software levels is paramount to success
- GRC solution sizing is based on the SAP NetWeaver platform and solution experience; SOD risk tables for Access Control require important storage consideration
- Performance of analytics processing of a running GRC system can improve by considering the techniques provided
- Understand the Access Control Rule Set and the impact it has on performance and disk storage during Analysis
- How you schedule and monitor the jobs can help keep the system in good running condition
- Technical Tips provided are valuable information for supporting the operation of the GRC system
Your Turn!

Questions?

How to contact me:
Kurt Hollis
kuhollis@deloitte.com
@kuhollis

Please remember to complete your session evaluation