Securing GRC - designing effective security within GRC Access Control

Sergiy Mysyk
▪ Understanding of SAP GRC Authorization System
▪ Approach to designing security within Access Control
▪ How to restrict access beyond roles and authorization objects - customizing GRC end user interface
Introduction to SAP GRC Access Control security
Leading practice of designing GRC AC Security that segregate access within GRC but still meet your business requirements
Access control beyond roles: how to control what users can view and change by modifying user interface
Wrap up and questions
GRC AC AUTHORIZATION BASICS

GRC AC 10.0 is an ABAP based system and uses standard SAP Netweaver authorization system.

Security roles are maintained through PFCG and assigned directly to user master records – SU01
End User Interface and SAP Roles

- Netweaver Business Client (NWBC) is the “front end” user interface and is accessed via internet browser
- Security roles are maintained through PFCG on the “backend” – SAP GUI
- Roles and authorizations within them control what is visible and what the user can do within each application (webdynpro) in NWBC
Introduction to SAP GRC AC Security

NWBC Work Center Access

- The Menu tab of a PFCG role and the folders within it control the Work Centers (folders) that are displayed in NWBC.
- Does not provide authorizations.
- Contents of each standard SAP delivered work center can be modified by changing the Launch Pad (next section).

Follow @ASUG365 and #ASUG2013 on Twitter
• You can also directly add individual web dynpro applications in place of a launch pad
Access Within GRC AC Work Centers, cont

- Cross Application Authorization Object CA_POWL restricts access to the entire POWL* iViews within the NWBC tabs (similar to S_TCODE)

<table>
<thead>
<tr>
<th>Authorization Object Technical Name</th>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA_POWL</td>
<td>POWL_APPID</td>
<td>GRAC_SOD_FUNCTION</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GRAC_SOD_RULESET</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GRAC_SODRISK</td>
</tr>
</tbody>
</table>

*POWL – Personal Object Work List
Access Within GRC AC Work Centers, cont.

- GRC authorization objects can further restrict access on individual webdynpro applications.
Additional Examples of Authorization Objects

- Restricting Access to certain types of sensitive reports, such as Firefighter Log reports is normally required. Object GRAC_REP controls access to the various reporting links.

<table>
<thead>
<tr>
<th>Report Id</th>
<th>Report Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRAC_SPM_CLOGS</td>
<td>Consolidated Log Report</td>
</tr>
<tr>
<td>GRAC_SPM_INVALID_SU</td>
<td>Invalid Superuser Report</td>
</tr>
<tr>
<td>GRAC_SPM_FFLOG_SUM</td>
<td>Firefighter Log Summary</td>
</tr>
<tr>
<td>GRAC_SPM_RCODE_ACTVT</td>
<td>Reason Code and Activity Report</td>
</tr>
<tr>
<td>GRAC_SPM_TXN_LOG</td>
<td>Transaction Log and Session Details</td>
</tr>
<tr>
<td>GRAC_SPM_SOD_REPORT</td>
<td>SOD Conflict Report for Firefighter IDs</td>
</tr>
</tbody>
</table>

- Additional security available through other GRAC objects.
- Reports may appear under multiple Launch Pads.
Introduction to SAP GRC Access Control security

Leading practice of designing GRC AC Security that segregate access within GRC but still meet your business requirements

Access control beyond roles: how to control what users can view and change by modifying user interface

Wrap up and questions
• SAP provides standard-delivered roles that can be used as starting point

- SAP_GRAC_ACCESS_APPROVER
- SAP_GRAC_ACCESS_REQUEST_ADMIN
- SAP_GRAC_ACCESS_REQUESTER
- SAP_GRAC_ALERTS
- SAP_GRAC_ALL
- SAP_GRAC_BASE
- SAP_GRAC_CONTROL_APPROVER
- SAP_GRAC_CONTROL_MONITOR
- SAP_GRAC_CONTROL_OWNER
- SAP_GRAC_DISPLAY_ALL
- SAP_GRAC_END_USER
- SAP_GRAC_FUNCTION_APPROVER
- SAP_GRAC_NWBC
- SAP_GRAC_REPORTS
- SAP_GRAC_RISK_ANALYSIS
- SAP_GRAC_RISK_OWNER
- SAP_GRAC_ROLE_MGMT_ADMIN
- SAP_GRAC_ROLE_MGMT_DESIGNER
- SAP_GRAC_ROLE_MGMT_DESINGER
- SAP_GRAC_ROLE_MGMT_ROLE_OWNER
- SAP_GRAC_ROLE_MGMT_USER
- SAP_GRAC_RULE_SETUP
- SAP_GRAC_SETUP
- SAP_GRAC_SPM_FFID
- SAP_GRAC_SUPER_USER_MGMT_ADMIN
- SAP_GRAC_SUPER_USER_MGMT_CNTLR
- SAP_GRAC_SUPER_USER_MGMT.Owner
- SAP_GRAC_SUPER_USER_MGMT_USER
• The leading practice is to create a matrix of all the available web applications and future roles
• A role design workshop can be held with the business to customize the GRC roles
• Logically group functionality and consider assignment flexibility - because of the limited functionality of the SAP GRC AC as compared to SAP ECC task based vs. job based roles are normally not a concern

• Consider Segregation of Duties (SOD) risks within SAP GRC Access Control tool itself

SOD Examples:
• Creating mitigating controls and approving their assignment?
• Being a Firefighter Owner/approving Firefighter access and being able to create Firefighter IDs?
- Use the design workshop output to create a list of applicable SAP GRC Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>My Home</th>
<th>Access Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAM Security Administrator</td>
<td>D U D D</td>
<td>U U</td>
</tr>
<tr>
<td>EAM Controller</td>
<td>D U D D</td>
<td>U U</td>
</tr>
<tr>
<td>EAM Firefighter Owner</td>
<td>D U D D</td>
<td>U U</td>
</tr>
<tr>
<td>EAM Firefighters</td>
<td>D D D D</td>
<td>U U</td>
</tr>
<tr>
<td>BRM Business User</td>
<td>D D D D</td>
<td>U U</td>
</tr>
<tr>
<td>BRM Security Administrator</td>
<td>D U D D</td>
<td>U U</td>
</tr>
<tr>
<td>ARA Security Administrator</td>
<td>D U D D</td>
<td>U U</td>
</tr>
<tr>
<td>ARA Business User</td>
<td>D D D D</td>
<td>U U</td>
</tr>
<tr>
<td>Mitigating Control Owner</td>
<td>D U D D</td>
<td>U U</td>
</tr>
<tr>
<td>Risk Owner</td>
<td>D U D D</td>
<td>U U</td>
</tr>
<tr>
<td>Coordinator</td>
<td>D D D D</td>
<td>U U</td>
</tr>
<tr>
<td>Mitigation Monitor</td>
<td>D D U D</td>
<td>U D D D</td>
</tr>
<tr>
<td>ARM Requestor</td>
<td>D D U U</td>
<td>U D D D</td>
</tr>
<tr>
<td>ARM Administrator</td>
<td>D U D D</td>
<td>U D D D</td>
</tr>
<tr>
<td>ARM Security Administrator</td>
<td>D U D D</td>
<td>U D D D</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Roles</th>
<th>Role Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZS:GRAC:EAM:SECURITY_ADMIN</td>
<td>IT: GRAC EAM Administrator Role</td>
</tr>
<tr>
<td>ZS:GRAC:EAM:FF_CONTROLLER</td>
<td>IT: GRAC EAM Controller Role</td>
</tr>
<tr>
<td>ZS:GRAC:EAM:FF_OWNER</td>
<td>IT: GRAC EAM Owner Role</td>
</tr>
<tr>
<td>ZS:GRAC:EAM:FF_USER</td>
<td>IT: GRAC EAM Firefighter Role</td>
</tr>
<tr>
<td>ZS:GRAC:EAM:FF_ID</td>
<td>IT: GRAC EAM Firefighter ID Role</td>
</tr>
<tr>
<td>ZS:GRAC:BRM:BUS_USER_DSP</td>
<td>IT: GRAC BRM Display access Role</td>
</tr>
<tr>
<td>ZS:GRAC:BRM:SECURITY_ADMIN</td>
<td>IT: GRAC BRM Security Administrator Role</td>
</tr>
<tr>
<td>ZS:GRAC:BRM:ROLE_OWNER</td>
<td>IT: GRAC BRM Owner Role</td>
</tr>
<tr>
<td>ZS:GRAC:ARA:SECURITY_ADMIN</td>
<td>IT: GRAC ARA Security Administrator Role</td>
</tr>
<tr>
<td>ZS:GRAC:ARA:BUS_USER_DSP</td>
<td>IT: GRAC ARA Display access Role</td>
</tr>
<tr>
<td>ZS:GRAC:ARA:AUDIT_MITCRL_APPRV</td>
<td>IT: GRAC ARA Audit Mitigating Controller Approver Role</td>
</tr>
<tr>
<td>ZS:GRAC:ARA:MITCRL_OWNER</td>
<td>IT: GRAC ARA Mitigating Control Owner Role</td>
</tr>
<tr>
<td>ZS:GRAC:ARA:RISKOWNER</td>
<td>IT: GRAC ARA Risk Owner Role</td>
</tr>
<tr>
<td>ZS:GRAC:ARA:SOD_REVIEW_COORD</td>
<td>IT: GRAC ARA Segregation of Duties (SoD) Review Coordinator Role</td>
</tr>
<tr>
<td>ZS:GRAC:ARA:MITCRL_MONITOR</td>
<td>IT: GRAC ARA Mitigating Monitor Role</td>
</tr>
<tr>
<td>ZS:GRAC:ARM:UAR_COORD</td>
<td>IT: GRAC ARM User Access Review Coordinator Role</td>
</tr>
<tr>
<td>ZS:GRAC:ARM:ACCESS_REQUESTOR</td>
<td>IT: GRAC ARM Access Requestor Role</td>
</tr>
<tr>
<td>ZS:GRAC:ARM:ADMIN</td>
<td>IT: GRAC ARM Administrator Role</td>
</tr>
</tbody>
</table>
• When building GRC roles, authorization objects will be added manually
• Positive and negative testing should be conducted during UAT
AGENDA

- Introduction to SAP GRC Access Control security
- Leading practice of designing GRC AC Security that segregate access within GRC but still meet your business requirements
- Access control beyond roles: how to control what users can view and change by modifying user interface
- Wrap up and questions
It may be required to customize the end user interface to further restrict access where it is not possible via authorizations alone –

- Authorization object GRAC_BGJOB with any values makes the following two applications visible. Only viewing the jobs – “Background Jobs” and not scheduling – “Background Scheduler” is desired

Access may be restricted by creating a **custom** Access Management Launch Pad without the link “Background Scheduler”
Customizing GRC AC Launch Pads

- GRC administrators can add, remove, or move links on the SAP GRC v10.0 Launch pad or work center.
- SPRO -> GRC -> General Settings -> Maintain Customer Specific Menus -> Configure Launchpad for Menus
- Or transaction code LPD_CUST
- GRC uses 1 repository for all GRC applications and 7 Launch Pads. 1 for each workcenter.
• Role – specifies who can use the launch pad. Together with the instance, it uniquely defines the launch pad.

• Instance- Specifies what purpose the launch pad is used for.

• Repository – flag indicates if launch pad is a repository (i.e. collection of launch pads)

• Embedded – Indicates if workcenter is embedded within another workcenter.

• User Interface Building Block for FPM applications – most likely selections

• Change, Display and Delete icons to perform respective activity.
Step 1 – Create or Modify Launch Pad

- Open existing Launch Pad by double clicking
- Choose Launch Pad - Save-As
- Fill in attributes
- Right click items to Hide, Disable, Rename, etc
- To add a link from existing application click the Link to a Repository Application
Step 2 - Moving Links From Repository

- Double click `GRCIAPREOS`
- Expand `GRC_AccessControl`
- Click and drag existing application to folder structure
Step 2 - Adding a URL, optional

- Right-click a folder and select New Application
- Select URL from the drop down
- Click the Change icon next to URL
- Enter URL including http://
- Click SAVE. By default it will be inactive. Right click and choose Set Visible as a Quick Link
Modifying GRC AC User Interface

Step 3 – Create Webdynpro Components – FPM UIBB

- Required if want to create NEW workcenter
- FPM – Floor Plan Manager; UIBB – Universal Building Block
- SE80 – Locate the UIBB LPD components under Component Configuration
- Double click and then choose Start Configurator
- Select COPY
- Enter name for configuration and description
- Package should be Customer package or Local (if not transporting)
Step 4 - Associate FPM UIBB with Launch Pad

- Choose Change
- Click Goto Component Configuration
- Click Configure UIBB (sandbox has errors which is why not showing the custom configuration)
Step 4 - Associate FPM – UIBB with Launch Pad, cont.

- Click Launchpad
- Set the Launchpad by choosing the combination of Role and Instance
Modifying GRC AC User Interface

- SE80 – Locate the FPM - CC components under Application Configuration
- Double click and then choose Start Configurator
- Select COPY
- Enter name for configuration and description
- Package should be Customer package or Local (if not transporting)
Modifying GRC AC User Interface

Step 6 – Change Attributes of Component Configuration

- Choose Change
- Click Goto Component Configuration
- Click Attributes under the HOME section in the right panel
- Change the configuration name to the FPM-UIBB configuration from the prior step
Step 7 - Create Web Dynpro Components – Application Configuration

SE80 – Locate the FPM_AC components under Application Configuration

Double click and then choose Start Configurator

Select COPY

Enter name for configuration and description

Package should be Customer package or Local (if not transporting)
Step 7 - Create Web Dynpro Components – Application Configuration, cont.

- Click the change button of the newly copied AC configuration
- Change the configuration to the newly created Component Configuration created in step 6
Modifying GRC AC User Interface

Step 8— Associate PFCG Role with Launch Pad

- Transaction code PFCG
- Best to copy an existing role
- Right click item in Menu and choose Details
- Select the Application Configuration created in Step 7
Modifying GRC AC User Interface

Administratively Changing Text and Hiding Links

- Individual links and text may be changed/hidden system wide to suit your needs
- Locate Webdynpro application by right-clicking the page you wish to modify and select More Field Help
- Locate the Web Dynpro Component
- If you see Launch Pad or LPD, use the previous method

Follow @ASUG365 and #ASUG2013 on Twitter
Modifying GRC AC User Interface

Administratively Changing Text and Hiding Links

- Transaction code SE80
- Use Repository Browser or Repository Information System to location configuration object
- Package is typically GRAC_ACCESS_REQUEST
- Double click folder
- From the menu bar – Webdynpro Application-> Test – In Browser - Admin Mode
- This will launch an IE window
Modifying GRC AC User Interface

Administratively Changing Text and Hiding Links

- Notice admin mode
- Right click area you wish to change
- Select Settings for Current Configuration
Modifying GRC AC User Interface

Administratively Changing Text and Hiding Links

1. Hide links by changing to Invisible
2. Change the text that appears when hovering over a link
3. Change the text of a link
   - Click SAVE and CLOSE
   - Enter transport information

Follow @ASUG365 and #ASUG2013 on Twitter
Modifying GRC AC User Interface

Administratively Changing Text and Hiding Links

• Some applications may require an additional parameter to be included in the URL upon entering the Admin Mode

• GRAC_OIF_REQUEST_APPROVAL application, for example, requires a dummy request number to open in Admin mode, otherwise an error is displayed

• To avoid the error add a dummy instance of an object, such as access request - &OBJECT_ID=ACCREQ/123
End User Personalization Restriction

- By default end users are allowed to personalize their interface.
- This can pose a risk, especially when shared users are used (e.g. End User Logon Page).
- The permission can be restricted in “wd_global_setting” service in SICF.
End User Personalization Restriction

- Start Transaction SICF
- Drill down to \default_host/sap/bc/webdynpro/sap/ and right click on WD_GLOBAL_SETTINGS, click Test Service
- You can globally disable the setting that allows end users to personalize their screens
AGENDA

- Introduction to SAP GRC Access Control security
- Leading practice of designing GRC AC Security that segregate access within GRC but still meet your business requirements
- Access control beyond roles: how to control what users can view and change by modifying user interface
- Wrap up and questions
SAP GRC 10.0 is an ABAP system and users ABAP authorization objects to control access

Standard SAP Delivered Roles Should be Customized as per your Requirement

  - Role Folder Structure, Authorization to access specific POWL as well as other GRC authorization objects determine what the user sees or has access to in NWBC

You can customize or create your own individual work centers due to business or security requirements

You can administratively customize end user interface within NWBC and disallow end users to do the same
Follow @ASUG365 and ASUG CEO Bridgette Chambers @BChambersASUG on Twitter to keep up to date with everything at ASUG.

Follow the ASUGNews team of Tom Wailgum: @twailgum and Courtney Bjorlin: @cbjorlin for all things SAP.
THANK YOU FOR PARTICIPATING

Please provide feedback on this session by completing a short survey via the event mobile application.

SESSION CODE: 0907

For ongoing education on this area of focus, visit www.ASUG.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2013 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.