Role Optimization and Reduction using SAP GRC Role Management

Chris Radkowski, SAP GRC
Learning Points

- Task based versus job based role design
- SAP GRC Business Role Management Reporting
- Learn about new GRC Role Analytics
Agenda

Introduction
Terminology
Task Based Role Design
SAP GRC Business Role Management
Reporting Features in GRC10
GRC Role Analytics
Wrap Up
Role Management Topics

Role Design for Efficiency, Simplicity, and Sustainability

TASK BASED ROLE DESIGN

IT To Business Transformation

SAP ERP Security

ERP Consolidation

GRC Role Analytics
Agenda

Introduction

**Terminology**

Task Based Role Design

SAP GRC Business Role Management

Reporting Features in GRC10

GRC Role Analytics
role (rōl) n.

1. A character or part played by a performer. 2. The characteristic and expected social behavior of an individual. 3. A function or position.
Trends

- Organizations have implemented many roles as part of individual projects
- Inconsistency in role design as led to inefficiencies
- A simpler and more sustainable approach is necessary
- Examples show 80-90% reduction in roles, simpler administration of access, reduced SoDs
- But, existing roles are difficult to analyze and re-design….
- Trend toward task based role methodology
Entitlement vs. Function – what is a role?

For technical systems, roles can mean both an entitlement (*authorization*) and a *function* in a business process or organization. Unfortunately the terms aren’t consistently applied.

- SAP Single Role - Tcode, transaction, authorization, auth object
- Composite Role
- Business Role
- Position
- Task based Role
- Job Based Role
- Virtual Composite Role
- Group
- Function
- Enabler roles

Our roles change during the day in everyday life!
Agenda

Introduction
Terminology
Task Based Role Design
SAP GRC Business Role Management
Reporting Features in GRC10
GRC Role Analytics
Wrap Up
Task Based Design - SAP Security Complexity

- ±120,000 T-codes (SAP ERP 6.0) each with unique security/authorization checks
- ±2,700 standard authorization objects
- Functions can be accessed through multiple T-codes -
- Descriptions of SAP T-codes may not be representative
### Job vs. Task-Based Roles

#### Job-Based Approach
- Security is built based on positions/jobs for a group of users (e.g., Accounts Payable Manager)
- Provisioning based on Job responsibilities
- Smaller number of roles per user – increased risk for granting functionality more than once
- Transaction codes and authorizations typically duplicated in many roles
- Users may be granted more access than necessary as a result of “additional job” or backup responsibilities

#### Task-Based Approach
- Security is built based on small, definable tasks executed by a user (e.g., Process Cash Receipts)
- Larger number of roles per user – decreased risk of duplicate access
- Transaction codes in one role with very minimal exception
- User assignment flexibility – simple to grant additional access to only the tasks necessary
- Supports future growth and sustainability – role modification minimized as a result of functionality improvements and rollouts
Multi-Tier Role Design Methodology

**USER PROFILE**

- **TIER 1: GENERAL ACCESS**
  Common low risk system related tasks such as inbox, printing, SU53, etc.

- **TIER 2: DISPLAY ACCESS**
  Defined by functional area or organization that allow display and reporting access

- **TIER 3: FUNCTIONAL ACCESS**
  Activities that are the lowest common denominator of tasks and permission components to suit the needs of the end users. These are SOD free and part of a sub-process such as Invoice Processing or Material Master Maintenance.

- **TIER 4: CONTROL POINTS (Enablers)**
  Roles that provide the control point access or granularity needed by Tiers 1-3 such as Company Code, Plant, etc.
Job vs. Task Based Role Example

**Who**
- **Activity Roles**

**What**
- **Jobs**
  - 39 Roles/1,254 Update Transactions

**Where**
- **Organizational or Country Boundaries**

**Tasks**
- 12 Total Roles/37 Update Transactions

**Enabler Roles**
- All Organizations
Agenda

Introduction
Terminology
Task Based Role Design

**SAP GRC Business Role Management**

Reporting Features in GRC10
GRC Role Analytics

Wrap Up
Introducing Business Roles
# Role Search

## Search Criteria
- **Maximum number of result rows:** 100
- **Saved Variants:**

## Table
<table>
<thead>
<tr>
<th>Landscape</th>
<th>Role Type</th>
<th>Description</th>
<th>Business Process</th>
<th>Subprocess</th>
<th>Application Type</th>
<th>Current Phase</th>
<th>Project Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRC BI Maintenance Landscape</td>
<td>Single</td>
<td></td>
<td>PROCURE TO</td>
<td>ACCOUNTS P</td>
<td>SAP_ERP</td>
<td>Complete</td>
<td>SAP User Roles from DCM800</td>
</tr>
<tr>
<td>GRC BI Maintenance Landscape</td>
<td>Single</td>
<td></td>
<td>PROCURE TO</td>
<td>ACCOUNTS P</td>
<td>SAP_ERP</td>
<td>Complete</td>
<td>SAP User Roles from DCM800</td>
</tr>
<tr>
<td>GRC Development Landscape</td>
<td>Single</td>
<td>Accounts Payable Manager</td>
<td>Procure to Pay</td>
<td>Accounts Payable</td>
<td>SAP</td>
<td>Complete</td>
<td>SAP User Roles from DCM800</td>
</tr>
<tr>
<td>GRC Development Landscape</td>
<td>Single</td>
<td>Vendor Maintenance</td>
<td>Procure to Pay</td>
<td>Accounts Payable</td>
<td>SAP</td>
<td>Complete</td>
<td>SAP User Roles from DCM800</td>
</tr>
<tr>
<td>GRC Development Landscape</td>
<td>Derived</td>
<td>Vendor Maintenance Derived</td>
<td>Procure to Pay</td>
<td>Accounts Payable</td>
<td>SAP</td>
<td>Complete</td>
<td>SAP User Roles from DCM800</td>
</tr>
<tr>
<td>GRC Development Landscape</td>
<td>Single</td>
<td>MM PO and Vendor Maintenance Role</td>
<td>Procure to Pay</td>
<td>Accounts Payable</td>
<td>SAP</td>
<td>Complete</td>
<td>SAP User Roles from DCM800</td>
</tr>
<tr>
<td>GRC Development Landscape</td>
<td>Single</td>
<td>Vendor Master Maintenance</td>
<td>Procure to Pay</td>
<td>Accounts Payable</td>
<td>SAP</td>
<td>Complete</td>
<td>SAP User Roles from DCM800</td>
</tr>
<tr>
<td>GRC BI Maintenance Landscape</td>
<td>Single</td>
<td></td>
<td>PROCURE TO</td>
<td>VENDOR MI</td>
<td>SAP_ERP</td>
<td>Complete</td>
<td>SAP User Roles from DCM800</td>
</tr>
</tbody>
</table>
Agenda

Introduction
Terminology
Task Based Role Design
SAP GRC Business Role Management

**Reporting Features in GRC10**

GRC Role Analytics

Wrap Up
SAP Role Management Reports

Role Management Reports

*View details related to management of roles*

**Quick Links**
- List Action in Roles
- Compare Action in Menu and Authorization
- Compare User Roles
- User to Role Relationship
- Role Relationship with User / User Group
- PFCG Change History
- Master to Derived Role Relationship
- Single to Composite Role Relationship
- Role by date of generation
- Risk Terminator Log Report

Security Reports

*View details related to user, role, and profile security*

**Quick Links**
- Action Usage by User, Role and Profile
- Count authorization in Roles
- Count authorization for Users
- List Expired and Expiring Roles for Users
**User to Role Assignment Report**

Shows the list of users for each role.

### User to Role Relationship

#### Analysis Criteria

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Role Description</th>
<th>Profile Name</th>
<th>User</th>
<th>Valid From</th>
<th>Valid To</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>VS:FI_ACCOUNTS_MANAGER</td>
<td>Accounts Payable Manager</td>
<td>T13550487</td>
<td>Carl Novitsky (CNOVITSKY)</td>
<td>10/25/2007</td>
<td>12/31/2009</td>
<td>DCM</td>
</tr>
<tr>
<td>VS:FI_ACCOUNTS_MANAGER</td>
<td>Accounts Payable Manager</td>
<td>T13550487</td>
<td>Chris Smith (CSMITH)</td>
<td>10/25/2007</td>
<td>12/31/2009</td>
<td>DCM</td>
</tr>
<tr>
<td>VS:FI_ACCOUNTS_MANAGER</td>
<td>Accounts Payable Manager</td>
<td>T13550487</td>
<td>Cathryn Turner (CTUMBER)</td>
<td>10/25/2007</td>
<td>12/31/2009</td>
<td>DCM</td>
</tr>
<tr>
<td>VS:FI_ACCOUNTS_MANAGER</td>
<td>Accounts Payable Manager</td>
<td>T13550487</td>
<td>Cheryl Yukadin (CYUKADIN)</td>
<td>10/25/2007</td>
<td>12/31/2009</td>
<td>DCM</td>
</tr>
<tr>
<td>VS:FI_ACCOUNTS_MANAGER</td>
<td>Accounts Payable Manager</td>
<td>T13550487</td>
<td>Cindy Wighty (CWIGHTLY)</td>
<td>10/25/2007</td>
<td>12/31/2009</td>
<td>DCM</td>
</tr>
<tr>
<td>VS:FI_ACCOUNTS_MANAGER</td>
<td>Accounts Payable Manager</td>
<td>T13550487</td>
<td>Dan Brier (DBRIER)</td>
<td>10/25/2007</td>
<td>12/31/2009</td>
<td>DCM</td>
</tr>
<tr>
<td>VS:FI_ACCOUNTS_MANAGER</td>
<td>Accounts Payable Manager</td>
<td>T13550487</td>
<td>Dan Chabot (DCHABOT)</td>
<td>10/25/2007</td>
<td>12/31/2009</td>
<td>DCM</td>
</tr>
<tr>
<td>VS:FI_ACCOUNTS_MANAGER</td>
<td>Accounts Payable Manager</td>
<td>T13550487</td>
<td>Darra Duggan (DDUGGAN)</td>
<td>10/25/2007</td>
<td>12/31/2009</td>
<td>DCM</td>
</tr>
<tr>
<td>VS:FI_ACCOUNTS_MANAGER</td>
<td>Accounts Payable Manager</td>
<td>T13550487</td>
<td>Darla Gromlick (DGROMLIC)</td>
<td>10/25/2007</td>
<td>12/31/2009</td>
<td>DCM</td>
</tr>
<tr>
<td>VS:FI_ACCOUNTS_MANAGER</td>
<td>Accounts Payable Manager</td>
<td>T13550487</td>
<td>Dan Hallmark (DHALLMARK)</td>
<td>10/25/2007</td>
<td>12/31/2009</td>
<td>DCM</td>
</tr>
<tr>
<td>VS:FI_ACCOUNTS_MANAGER</td>
<td>Accounts Payable Manager</td>
<td>T13550487</td>
<td>Dan Hill (DHILL)</td>
<td>10/25/2007</td>
<td>12/31/2009</td>
<td>DCM</td>
</tr>
</tbody>
</table>
## Compare User Role Assignments

The image shows a user interface for comparing user role assignments. It highlights the need to add, keep, or remove roles between source and target users. The interface includes a table with columns for **Action**, **Role Name**, and **Role Description**.

Here are some examples of role assignments:

- **ADD**
  - JIRSAQ_VFAT_ADMINISTRATOR: Firefighter Administrator Role with full access
- **KEEP**
  - JIRSAQ_VFAT_ID_OWNER: Firefighter FireID owner's role
- **REMOVE**
  - GRC_PFCG: GRC PFCG Authorization
  - VS_FI_AP_INVOICES: InOut Invoices
- **ADD**
  - VS_FI_VMI_MAINTENANCE: Vendor Master Maintenance

This tool helps in maintaining consistent role assignments across different user profiles, ensuring that the necessary permissions are correctly assigned and managed.
### List of Actions in Roles

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Role Type</th>
<th>Role Description</th>
<th>Associated Role</th>
<th>Business Process</th>
<th>Landscape</th>
<th>Action</th>
<th>Action Description</th>
<th>Subprocess</th>
<th>Application Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-43</td>
<td>Enter Vendor Invoice</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_INVOICE_PROCESSING</td>
<td>Single</td>
<td>Procure Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-44</td>
<td>Clear Vendor</td>
<td>Accounts Receivable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-45</td>
<td>Clear Vendor</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-46</td>
<td>Item with Clearing</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-47</td>
<td>Pay With Clearing</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-48</td>
<td>Pay Outgoing Payments</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-49</td>
<td>Payment Request</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-50</td>
<td>Pay Vendor Invoice</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>SAP_FLAP_PAYMENT_CHECKS</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-51</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>SAP_FLAP_PAYMENT_CHECKS</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-52</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-53</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-54</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-55</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-56</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-57</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-58</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-59</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-60</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-61</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-62</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-63</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-64</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
<tr>
<td>VS:FLAP_ACCOUNTANT</td>
<td>Single</td>
<td>Process Vendor Invoices</td>
<td></td>
<td>Procure to Pay</td>
<td>ORC ERP Landscape</td>
<td>F-65</td>
<td>Parameters for Automatic Payment</td>
<td>Accounts Payable</td>
<td>SAP</td>
</tr>
</tbody>
</table>

Results are sortable and exportable.
Action Usage by User, Role, and Profile

- Configurable search query
- Multiple systems, ranges, wildcards
- User, Role, Profile
Action Usage by User, Role, and Profile

<table>
<thead>
<tr>
<th>System</th>
<th>Action</th>
<th>Action Description</th>
<th>User</th>
<th>User Name</th>
<th>Execution Count</th>
<th>Last Executed on</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCM</td>
<td>XK02</td>
<td>Change vendor (centrally)</td>
<td>CS15679O</td>
<td>Sateesh Venkata</td>
<td>7</td>
<td>03/28/2012 04:48:01</td>
</tr>
<tr>
<td>DCM</td>
<td>XK02</td>
<td>Change vendor (centrally)</td>
<td>D022589</td>
<td>Frank Mueller</td>
<td>20</td>
<td>02/23/2012 16:40:48</td>
</tr>
<tr>
<td>DCM</td>
<td>XK02</td>
<td>Change vendor (centrally)</td>
<td>FF_VENDORS</td>
<td>Firefighter Vendor Maintenance</td>
<td>50</td>
<td>05/03/2011 16:53:47</td>
</tr>
<tr>
<td>DCM</td>
<td>XK02</td>
<td>Change vendor (centrally)</td>
<td>B11050</td>
<td>B11050</td>
<td>18</td>
<td>03/22/2011 20:38:47</td>
</tr>
<tr>
<td>DCM</td>
<td>XK02</td>
<td>Change vendor (centrally)</td>
<td>MLAW</td>
<td>Megan Law</td>
<td>2</td>
<td>04/04/2011 20:20:50</td>
</tr>
</tbody>
</table>
Agenda

Introduction
Terminology
Task Based Role Design
SAP GRC Business Role Management
Reporting Features in GRC10

**GRC Role Analytics**

Wrap Up
GRC Role Analytics
Agenda

Introduction
Terminology
Task Based Role Design
SAP GRC Business Role Management
Reporting Features in GRC10
GRC Role Analytics

Wrap Up
Key Learnings

- SAP GRC Business Role Management comprehensive and powerful reporting features to deliver insights into existing assignments and activities
- Business role management can help implement a task based role methodology
- Task based role methodologies can reduce the number of roles up to 90%, simplify provisioning and reduce SoDs.
- SAP GRC is focused on delivering new role analytics tools
Thank You! – Questions?
Additional Resources and References

- GRC Insider 2012 - Drive Cost Savings Through a Practical Approach for Designing and Implementing Business Process- and IT-Based Roles - Jason Glantz and Shivraj Patil Ernst & Young
- GRC Insider 2012 - Resolve Segregation of Duties and Access Violations with a Cost-Effective, Task-Based Approach to Security - Raymond Mastre, PricewaterhouseCoopers
- GRC Insider 2012 - Case Study: How Coca-Cola Reduced the Number of Roles Within Its SAP Landscape by 90% - Kyleen Wissell, The Coca-Cola Company
- JAVA / Enterprise Portal Content Naming Convention and ABAP Role Design Document Updated: July 11, 2010 - Larry Justice

SAP GRC10 Business Role Management – Managing your role design with SAP GRC10
www.sdn.sap.com/irj/bpx/go/portal/prtroot/docs/library/uuid/80063a8e-1da6-2e10-aaa5-fda1f0936c37
Thank you for participating.

Please remember to complete and return your evaluation form following this session.

For ongoing education on this area of focus, visit the Year-Round Community page at www.asug.com/yrn