Auditing SAP GRC

ISACA-August 17, 2012
Introductions

Sean Campbell

Sean Campbell is an IT Auditor at The Coca-Cola Company. His experience has focused primarily around IT compliance and SAP security. Prior to joining Coca-Cola, Sean was an IT Auditor with KPMG and Fiserv where he led SAP audits and gained experience in financial services.

Sean holds a Bachelor’s Degree in Management Information Systems and a MBA, both from the University of Georgia. Sean also holds a CISA certification.

Jay Gohil

Jay Gohil is an IT Auditor at The Coca-Cola Company. His experience has focused primarily around IT compliance and SAP security. Prior to joining Coca-Cola, Jay was a consultant with Protiviti where he led several projects integrating the SAP GRC Access Controls Suite and assisted with segregation of duties analysis, user access design, and remediation of SAP security issues.

Jay holds a Bachelor’s Degree in Computer Engineering and a Master’s Degree in Decision and Information Sciences, both from the University of Florida. Jay also holds a CISA certification.
The Coca-Cola Company - Introduction

- ~46+ billion in sales
- 200+ countries where our beverages are sold
- 500+ brands of the Coca-Cola Company
  - 15 billion dollar brands
- 3,300+ different beverages
- 1.7+ billion servings per day
- With bottling partners, Coke ranks top 10 in private employers worldwide with more than 700,000 system employees (About 145,000 work for The Coca-Cola Company)
The Coca-Cola Company - Worldwide

2011 WORLDWIDE UNIT CASE VOLUME
GEOGRAPHIC MIX

- 22% North America
- 29% Latin America
- 15% Europe
- 16% Eurasia & Africa
- 18% Pacific
Coke has three large instances based on business need and mergers (Global, CCR, BIG)
  - Many smaller instances run at bottler locations

Multiple landscapes established for different business processes (i.e. Primary-FiLo, HR, BW, etc.)

Largest landscapes have ~20,000 users
● SAP Security Overview
  - SAP Authorization Concept
  - Common Issues

● SAP GRC Overview
  - Modules
  - Risk and Function Overview
  - SAP Security Issues Addressed

● Auditing SAP GRC
  - Governance
  - Security
  - Configuration
  - Change Management
SAP Security Overview
SAP Security – Authorization Concept: Overview

User
Role
Profile
Authorization Objects
Authorization Fields
● When a user logs onto SAP all the authorization objects and fields that have been assigned to them through roles and profiles are loaded into their “user master” record

● When a user attempts to execute an action in SAP the authorization objects and fields from the user master are checked programatically

● Within the fields of the authorization objects a user can be restricted to:
  - Display vs. Maintain
  - Specific items classified by company codes (or many other groupings)
  - Many other restrictions based on individual objects
● Inheritance
  - Unintended access given to users due to unknown combinations of authorization objects through various roles

● Broad Access Designed in Roles
  - Ranges or wildcards assigned in authorization objects allows users access to functions for which they were not authorized

● Assignment of Roles with Broad Access
  - To grant a user access to a specific T-Code a SAP Security employee may assign a role that grants the user excessive access
● Segregation of Duties and Sensitive Access
  - Users could be given access that would result in segregation of duties risks or have access to powerful business or IT functions without authorization

● No Visibility into Potential Issues
  - No visibility into who has SoD conflicts or even sensitive access without a considerable manual data pull and analysis

● No Prevention of New Problems
  - No way to truly prevent assignment of roles that create inheritance issues or create SOD risks
SAP GRC Overview
## SAP GRC - History

<table>
<thead>
<tr>
<th>Virsa Systems</th>
<th>SAP GRC Access Control 5.3</th>
<th>SAP GRC Access Control 10.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefighter</td>
<td>Superuser Privilege Management</td>
<td>Emergency Access Management</td>
</tr>
<tr>
<td>Compliance Calibrator</td>
<td>Risk Analysis &amp; Remediation</td>
<td>Access Risk Analysis</td>
</tr>
<tr>
<td>Access Enforcer</td>
<td>Compliant User Provisioning</td>
<td>Access Request Management</td>
</tr>
<tr>
<td>Role Architect</td>
<td>Enterprise Role Management</td>
<td>Business Role Management</td>
</tr>
</tbody>
</table>

### Version 10:
- Customizing moved into SAP Reference IMG (SPRO)
- Centralized firefighter usage and workflow
  - Provides auditable process for tracking log review approvals
- All components are now ABAP based
- Improved risk analysis interface, allows filtering and sorting
### SAP GRC - Modules

<table>
<thead>
<tr>
<th>Access Risk Analysis (ARA)*</th>
<th>Emergency Access Management (EAM)*</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Real-time &amp; centralized SOD/sensitive access reporting and monitoring</td>
<td>• “Firefighter”</td>
</tr>
<tr>
<td>• Ruleset management</td>
<td>• Temporary elevated access</td>
</tr>
<tr>
<td>• User Access Simulation</td>
<td>• Track transaction code usage and changes</td>
</tr>
<tr>
<td>• Mitigating Controls</td>
<td>• Audit logs, email alerts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Request Management</th>
<th>Business Role Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Workflow</td>
<td>• Role documentation repository</td>
</tr>
<tr>
<td>• User Provisioning</td>
<td></td>
</tr>
</tbody>
</table>
● Risks
  - SOD Risks – Critical combination of 2 or more specific activities
  - Sensitive Access Risk – A risk that a user has access to a specific functional area

● Ruleset Concept
  - Rulesets are a grouping of risks
  - Risks are made up of function groups
  - Function groups are made up of multiple t-codes and/or objects

● Firefighter
  - Addresses segregation of duties concerns by providing temporary elevated access that is controlled and monitored
Segregation of Duties

Certain separate business processes and functions in The Coca-Cola Company, if executed by a single user, would present an unacceptable risk to the integrity of the Company’s processes, and could expose the Company to fraud risk. Therefore, incompatible duties of this type must be segregated and monitored.

Sensitive Access

Certain transactions or activities in The Coca-Cola Company are regarded as “sensitive” due to the following:

1) The transaction allows access to confidential information
2) The transaction should only be executed by select user(s) who are highly experienced and knowledgeable around the use of the transaction
3) The transaction, if executed inappropriately, would cause a significant (negative) impact to operations.
The Coca-Cola Company Rule Set

Maintain Purchase Orders Vs. Manage Goods Receipt

Maintain Purchase Orders
- ME21N – Create Purchase Order
- ME22N – Change Purchase Order
- Create PO for company codes
- Create PO for purchasing area

Manage Goods Receipt
- MIGO – Goods Movement
- MB01 – Post Goods Receipt on PO
- Create GR for company code
- Create GR for purchasing area
SAP GRC - User Interface

**SAP Business Client**

**Access Dashboards**
Explore dashboards for access risk analysis, business role management and user access management.
- Quick Links
- Access Rule Library
- Mitigating Control Library
- Risk Violations
- User Analysis
- Role Analysis
- Violations Comparisons
- Alerts
- Role Library
- Access Requests
- Access Provisioning
- Risk Violation in Access Request
- Service Level for Access Request

**Role Management Reports**
View details related to management of roles.
- Quick Links
- List Actions 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

**Access Risk Analysis Reports**
View details related to access risk analysis.
- Quick Links

**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
## SAP GRC - User Interface

### Risk Analysis: User Level

#### Multiple Selection

**Analysis Criteria**

- System
- User
- User Group
- Custom Group
- Risk Level
- Rule Set
- User Type

**Report Options**

- Format: Summary
- Type: Mitigate Risk

**Analysis Results**

**Result Set:** Result Set 1

**View:** Standard View

**Display As:** Table

**Format:** Summary

<table>
<thead>
<tr>
<th>User ID</th>
<th>Access Risk ID</th>
<th>System</th>
<th>Rule ID</th>
<th>Risk Level</th>
<th>Action</th>
<th>Last Executed On</th>
<th>Execution Count</th>
<th>Control</th>
<th>Monitor</th>
<th>Org Rule ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP06</td>
<td></td>
<td></td>
<td>002M</td>
<td>High</td>
<td>MR11SHOW</td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP06</td>
<td></td>
<td></td>
<td>002M</td>
<td>High</td>
<td>YDPRUIFD</td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP06</td>
<td></td>
<td></td>
<td>002M</td>
<td>High</td>
<td>MR11SHOW</td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP06</td>
<td></td>
<td></td>
<td>002M</td>
<td>High</td>
<td>YDPRUIFD</td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SM01</td>
<td></td>
<td></td>
<td>008I</td>
<td>High</td>
<td>S_P99_41000102</td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SM01</td>
<td></td>
<td></td>
<td>008I</td>
<td>High</td>
<td>ZLOCKBOX</td>
<td></td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Last Updated by [Name] at 27.06.2012 13:57:27 EST
Use of SAP GRC gives visibility into SOD issues, inheritance issues, and can prevent the assignment of roles that create issues

- Ability to validate that no violations of an SOD ruleset exist within single roles
- Identify and review sensitive access assigned to users
- Workflow can be implemented to require risk analysis to be completed prior to new role assignments (preventative control!)
● **Governance**  
  - Identifying and incorporating new functionality  
  - Establishing ownership of risks, roles and controls

● **Security**  
  - Limiting access to configure and make changes

● **Configuration**  
  - Key parameters are configured appropriately  
  - Changes are documented and monitored

● **Change Management**  
  - Ruleset changes (risks and functions) are authorized & approved
Auditing SAP GRC
Governance
Governance is important to the long term relevance of GRC
- Incorporates changes in the environment
- Establishes ownership and responsibility
- Drives remediation decisions

Key areas to consider for a governance team
- Ownership (GRC Risks, SAP Roles, Mitigating Controls)
- Risk Level of GRC Risks and Expectations
- New Functionality
● **Who approves access?**
  - Based on roles
  - Manager
  - GRC Risk
  - Who approves assigning a mitigating control

● **Who defines the risk/function and approves changes?**
  - What is included in a GRC risk/function (how is this determined)
  - What is the defined risk level
What does each risk level mean?
- Are users allowed to access certain transactions at all?
- What are the expectations for each risk level
  - # of violations
  - Remediation timeframe
What is the process to identify new functionality added to the system?
- T-Codes
- New Modules
- Custom & New Authorization Objects

How are these analyzed and included (if needed) into a ruleset?
● **Access Provisioning**
  - Preventative SOD/sensitive access analysis
  - Appropriate approvals (role owner, manager)

● **Periodic Access Reviews**
  - Detective SOD/sensitive access analysis

● **Mitigating Control Reviews**
  - Review of users with sensitive access based on business need
Auditing SAP GRC
Standard SAP Functionality
SAP GRC Version 10 runs on an ABAP landscape

- **Reviewing Sensitive Access**
  - User Management (SU01, PFCG, etc.)
  - Change Management (STMS, SCC4, etc.)
  - Configuration Management (SPRO, etc.)

- **Other relevant high risk areas should also be reviewed during an audit of the SAP systems**
Similar to previous “ABAP Security” slide, typical change management testing procedures for a SAP audit would apply as changes are moved in via transports

- Utilize T-Code STMS (Import Overview > Import History) to identify the population of transports released into production during the period under review within each in-scope landscape.

- As long as the client is locked, all configuration and risk/function changes must be transported.

- Verify client lock status and history with T000 table.
Auditing SAP GRC
Audit Risk Analysis (ARA)
ARA is the web front end interface into SAP GRC

● Delivered Roles
  - SAP_GRAC_ALL (application administrator role)
  - SAP_GRAC_SETUP (access to setup and customize GRC AC)
  - SAP_GRAC_RULE_SETUP (define and update rules)

● Restrict access to the GRC Administrator
Key Configuration

<table>
<thead>
<tr>
<th>Parameter Group</th>
<th>Parameter ID</th>
<th>Description</th>
<th>Default Value</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Analysis</td>
<td>1026</td>
<td>Default user type for risk analysis</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1028</td>
<td>Include Expired Users</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td></td>
<td>1029</td>
<td>Include Locked Users</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td></td>
<td>1030</td>
<td>Include Mitigated Users</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td></td>
<td>1031</td>
<td>Ignore Critical Roles and Profiles</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1032</td>
<td>Include Reference user when doing User Analysis</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1033</td>
<td>Include Role/Profile Mitigating Controls</td>
<td>YES</td>
<td></td>
</tr>
</tbody>
</table>

• All configuration is done via transaction SPRO
• Default values can be overridden!
**Other Key Configurations**

<table>
<thead>
<tr>
<th>Parameter Group</th>
<th>Parameter ID</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Log</td>
<td>1001</td>
<td>Enable Function Change Log</td>
<td>YES</td>
</tr>
<tr>
<td></td>
<td>1002</td>
<td>Enable Risk Change Log</td>
<td>YES</td>
</tr>
<tr>
<td></td>
<td>1003</td>
<td>Enable Organization Rule Log</td>
<td>YES</td>
</tr>
<tr>
<td></td>
<td>1004</td>
<td>Enable Supplementary Rule Log</td>
<td>YES</td>
</tr>
<tr>
<td></td>
<td>1005</td>
<td>Enable Critical Role Log</td>
<td>YES</td>
</tr>
<tr>
<td></td>
<td>1006</td>
<td>Enable Critical Profile Log</td>
<td>YES</td>
</tr>
<tr>
<td></td>
<td>1007</td>
<td>Enable Rule Set Change Log</td>
<td>YES</td>
</tr>
</tbody>
</table>
Risk Analysis: User Level

Analysis Criteria

- System
- User
- User Group
- Custom Group
- Risk Level
- Rule Set
- User Type

Report Options

- Format: Summary, Technical View
- Type:
  - Access Risk Analysis
  - Access Risk Assessment
  - Mitigation Analysis
- Additional Criteria:
  - Include Mitigated Risks
  - Show All Objects
  - Consider Org Rule
  - Offline Data

When was the last sync?

Save Variant as: [Field] [Save]
● **Ruleset Changes**
  - Report: Reports and Analytics > Audit Reports > Change Log Report
    - Filter: By Function, Risk, Rule Set, Organization Rule
    - Filter: Changed On field based on testing period

● **Changes should follow existing governance processes for authorization**
Auditing SAP GRC

Emergency Access Management (EAM)
EAM is Emergency Access Management module within SAP GRC. This is commonly referred to as firefighter.

- **Delivered Roles**
  - SAP_GRAC_SUPER_USER_MGMT_ADMIN (Administrator role)
## Key Configuration

<table>
<thead>
<tr>
<th>Parameter Group</th>
<th>Parameter ID</th>
<th>Description</th>
<th>Default Value</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency Access Management</td>
<td>4001</td>
<td>Default Firefighter Validity Period (Days)</td>
<td>&lt;blank&gt;</td>
<td>365</td>
</tr>
<tr>
<td></td>
<td>4002</td>
<td>Send E-mail Immediately</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4003</td>
<td>Retrieve Change Log</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4004</td>
<td>Retrieve System Log</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4005</td>
<td>Retrieve Audit Log</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4006</td>
<td>Retrieve O/S Command Log</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4007</td>
<td>Send Log Report Execution Notification Immediately</td>
<td>YES</td>
<td></td>
</tr>
</tbody>
</table>
Additional Review Items

- Analysis of Number of IDs, ID Owners, ID Controllers
  - **Key Reports**
    - Report: Setup > Superuser Assignment > Owners
    - Report: Setup > Superuser Assignment > Controllers
    - Report: Reports and Analytics > EAM Reports
  - **Analytics:**
    - Number of Unique Owners, Controllers
    - Superuser IDs With Same Owner and Controller
    - Number of Unique Superuser IDs Across All Systems/Clients
    - Top 5 Owners and Number of IDs Owned
    - Number of Logins Per Superuser ID
    - Time to Review Audit Logs
    - Number of Logs Per Controller
Common Audit Issues
SAP GRC
**Common Audit Issues**

- **Ruleset and Risk Changes**
  - Ruleset changes need valid documentation (i.e. authorization trace)
    - KEY POINT: Removing an item (like an authorization object) will generally make the rule more broad increasing false positives
  - Risk changes need consent from governance committees
    - Impact reporting and mitigating controls

- **Mitigating Controls** (Do not address the SOD risk)
  - Release PO vs. Edit PO Mitigating Control
    - Bad Example: Disbursements are approved before being paid. This would not address the risk because the PO was approved/released!
    - Good Example: Disbursements are reviewed to ensure users that modified PO were not the only user to approve/release the PO.
● **Business Process Changes**
  - Addressing functional SOD in business areas
  - Provisioning Access (single process, do not by-pass)
  - Remediation of conflicts
    • Periodic process or reliance on preventative controls?

● **Configurations**
  - Not configured to log all changes
  - Not reviewing locked users by default

● **Firefighter**
  - Excessive use
  - Excessive access
  - Broadly assigned
Questions?
Contact Information

Sean Campbell
secampbell@coca-cola.com

Jay Gohil
jgohil@coca-cola.com