GRC Access Control – Access Risk Management Guide

Applies to
SAP Solutions for Governance, Risk, and Compliance: GRC Access Control (comprising applications formerly known as Virsa Compliance Calibrator, Virsa Firefighter, Virsa Access Enforcer and Virsa Risk Terminator)

Summary
SAP’s solutions for Governance, Risk, and Compliance comprise GRC Access Control, an application that handles sustainable prevention of Segregation of Duties (SoD) violations. This paper outlines a proven approach to successfully manage to implement SoD risk analysis and remediation.

Author: Gary Dickhart, Susan Stapleton
Company: SAP

Authors’ Bio
Gary Dickhart manages the Customer Advisory Office of SAP’s business unit for Governance, Risk, and Compliance.

Susan Stapleton is a leading expert on GRC Access Control. Prior to joining the Customer Advisory Office for GRC, Susan gained her experience in a large number of GRC Access Control implementations.
## Implementation, Configuration and Training Schedule

### Task Set 1 / Week 1

<table>
<thead>
<tr>
<th>Task Set 1 / Week 1</th>
<th>Description</th>
<th>Required Attendees</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pre-workshop</strong></td>
<td>Pre-implementation phone calls and preparation</td>
<td>(Support), Access Control consultant, Customer technical contact</td>
</tr>
<tr>
<td></td>
<td>Installation in development/test system (DEV) (prior to Day 1)</td>
<td>Customer technical contact</td>
</tr>
<tr>
<td><strong>Day 1</strong></td>
<td>Installation verification &amp; security discussions</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>If not completed already, create roles in UME for GRC Access Control</td>
<td>Access Control consultant, Customer technical contact</td>
</tr>
<tr>
<td>2</td>
<td>System access and review of initial system settings. Installation verification (ensure java connectors have been configured and RTAs are loaded in target systems).</td>
<td>Access Control consultant, Customer GRC Access Control administrator(s)</td>
</tr>
<tr>
<td>3</td>
<td>Complete post-installation and configuration steps. Synchronization of data and rule loading of the delivered rule set. Customize GRC Access Control default settings and parameters. Discuss configuration and the impact of parameter settings on reports, analysis, and mitigation.</td>
<td>Access Control consultant, Customer GRC Access Control administrator(s)</td>
</tr>
<tr>
<td>4</td>
<td>Discussion of current security work strategy. Overview of delivered risk assumptions, organizational level analysis, best practices and SoD implications</td>
<td></td>
</tr>
<tr>
<td><strong>Day 2</strong></td>
<td>Knowledge transfer to GRC Access Control administrator(s) - Process for customizing rules, on-going maintenance activities</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Exercise for configuration review</td>
<td>Access Control consultant, Customer GRC Access Control administrator(s)</td>
</tr>
<tr>
<td>6</td>
<td>Verify all GRC Access Control query functionality and that results are returned as expected. Review layout and navigation for related to NetWeaver and GRC Access Control.</td>
<td>Access Control consultant, Customer GRC Access Control administrator(s)</td>
</tr>
<tr>
<td>7</td>
<td>Kickoff Meeting to review specific needs and goals of Customer and agenda for the two week engagement. (Key stakeholders in the implementation and the ongoing project). High level review of Customer’s existing Segregation-of-Duties (SOD) data and security processes, project timeline.</td>
<td>Access Control consultant, Customer GRC Access Control administrator(s), Customer security administrator, Project managers</td>
</tr>
<tr>
<td>Day 3</td>
<td>Customer SOD requirements analysis</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Rule Architect exercise</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Review SOD Management and ownership. Discuss rule assumptions and delivered SoDs for appropriateness. Review custom business processes, if applicable</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Discuss GRC Access Control reports (Executive, summary and detail and how to use each for SoD resolution.</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Mitigation documentation – steps to create administrators, business units, control definitions and assignment</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Tactics and approaches for integrating all stakeholders into SoD governance process</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Preparation or catch-up time as required to ensure week one tasks are completed.</td>
<td></td>
</tr>
</tbody>
</table>

**Day 4**

**Firefighter and 1st week Wrap up and next steps discussion**

| 16 | Mitigation exercise |
| 17 | Review risk management process outline to review material and roadmap for project next steps |
| 18 | Review GRC Access Control reports and discuss real cleanup scenarios for single roles. Role level reporting and analysis; simulation for proactive ongoing compliance. |
| 19 | All hands meeting, Mitigation & Firefighter, BPO Presentation |
| 20 | Firefighter implementation tasks and best practices for FF usage, log review and ongoing tasks |
| 21 | Firefighter Practical |

**Task Set 2 / Week 2**

**Pre-workshop**

<table>
<thead>
<tr>
<th>Preparation</th>
</tr>
</thead>
</table>

**Day 5**

Review of Project Status, User Reporting, Alerts
<table>
<thead>
<tr>
<th>Day 6</th>
<th>Detailed GRC Access Control Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>Mitigation in GRC Access Control. Discussion of best practices – Approvers, Monitors and documentation of controls</td>
</tr>
<tr>
<td>28</td>
<td>Continuation of building customized data into Rule Architect. Critical Action and Permission rules</td>
</tr>
<tr>
<td>29</td>
<td>Perform testing and validation of SOD reports based on the additional rules loaded.</td>
</tr>
<tr>
<td>30</td>
<td>Perform testing and validation on sensitive access reports based on the additional rules loaded in the product.</td>
</tr>
<tr>
<td>31</td>
<td>Prepare the Management, Executive, Summary, and Detail reports for the rules that have been loaded in GRC Access Control. Begin sizing user remediation effort.</td>
</tr>
<tr>
<td>32</td>
<td>Reporting exercise</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Day 7</th>
<th>Remediation strategy &amp; options analysis and Risk Terminator</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>Analysis of results to determine the extent of remediation required.</td>
</tr>
<tr>
<td>34</td>
<td>Workshop to discuss potential remediation methodologies that are appropriate to address the security violations identified.</td>
</tr>
<tr>
<td>35</td>
<td>Remediation exercise</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>36</td>
<td>Perform walkthroughs of the remediation strategies using live examples.</td>
</tr>
<tr>
<td>37</td>
<td>Risk Terminator Overview/Configuration settings and testing</td>
</tr>
<tr>
<td>Day 8</td>
<td>Remediation planning/Wrap-up of open items</td>
</tr>
<tr>
<td>38</td>
<td>Discuss next steps as required for management reporting, alerts usage, organizational rules, and other GRC Access Control functionality as needed.</td>
</tr>
<tr>
<td>39</td>
<td>Discuss recommendations for remediation strategies and methodologies that will facilitate the clean-up of security access violations.</td>
</tr>
<tr>
<td>40</td>
<td>Develop a remediation project plan including customized scheduling, estimation of work hours and milestones to report on.</td>
</tr>
<tr>
<td>41</td>
<td>Wrap-up session to include Q&amp;A and discussion of ongoing tasks for Customer</td>
</tr>
<tr>
<td></td>
<td>Post-implementation call to discuss any issues or questions in week proceeding services.</td>
</tr>
</tbody>
</table>
Implementation

Kick-off Meeting
An initial meeting with the principal client contact and other stakeholders determined by them should be held to go over plans for risk analysis and remediation. The consultant will spend time settling in to the facilities and reviewing the installation of the products.

This is also a good time to identify the client processes and system landscape to make sure the configuration and subsequent rule building and validation steps take into account the client’s requirements. The following are the major elements to be discussed:

1. Security processing
2. Audit findings related to Segregation-of-Duties (SOD)
3. Current projects
4. SAP system versions and landscape
5. Applicable players discussed in the SOD Management process

SOD Process, Roles and Responsibilities
Review the roles and responsibilities for the SOD management process. The purpose is to get concurrence from the personnel attending on the definition of terms and how the process can be applied to the client’s environment. The following topics are covered:

1. Segregation-of-Duties management process overview
2. Roles and responsibilities
3. Major phases and objectives of the process
4. Identify client environment

Segregation-of-Duties Management Process Overview
SAP security provides the opportunity to prevent an individual from executing combinations of transactions without the involvement of another person in the process. SOD proactive management involves identifying the ways to commit fraud or accidentally corrupt processes. This includes monitoring security privileges granted to individuals so capabilities are known before they are exploited.

However, there are circumstances which require the same person to be able to order and receive materials, for example. In these cases, a detective control should be put in place to review that person’s access to detect fraud or unusual activities. The management process is designed to help Business Process Owners (BPOs) recognize SOD risks and implement the necessary controls (mitigating controls).

Security owns the SOD process and acts as a facilitator. The BPOs are responsible for managing the risks and designing alternate controls when Segregation-of-Duties cannot be achieved. Once the risks are defined, Business Process Analysts (BPAs) provide the technical knowledge to ensure the appropriate transactions and related objects and field values are defined in GRC Access Control. Business Process Owners are also responsible for approving actions taken to rectify SOD issues inherent in roles under their responsibility.

The audit department is responsible for conducting audits to discover Segregation-of-Duties issues and for testing any mitigating controls implemented by business personnel. The SOD rule keeper is responsible for controlling the rules in security but not SAP Security administrator activities. The specific activities of all the participants are outlined in this document.
Roles and Responsibilities

**Business Process Owners (BPOs)** - staff responsible for protecting the integrity the information and processes supported by an IT system. BPOs are in charge of

- Identifying risk and/or approving controls for monitoring risks
- Approving remediation to address user access issues in the IT system
- Designing alternative controls to mitigate Segregation-of-Duties issues
- Communicating access assignments or role changes

**Senior executives** - approve or reject risks between business areas and approve mitigating controls for risks.

**SAP security** - owners of the SOD management process and associated software products who facilitate decision making as well as alternative methods to manage SOD risks.

**Business Process Analysts (BPAs)** - help security administrators define the technical rules for each business area for approved risk conditions and recommend alternatives to eliminate SOD risks in roles and user assignments.

**Internal audit** - perform risk assessments on a regular basis to identify new risks, perform periodic testing of rules and mitigating controls; act as a liaison with external auditors.

**SOD rule keeper** - maintains the rules in the development environment, promotes to the production environment for risk monitoring and is responsible for enforcing the process for building and gaining approval for the rules to be used.
## SOD Management Process Phases

<table>
<thead>
<tr>
<th>Phase</th>
<th>Steps</th>
<th>Reference Documents / Tools</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Recognition</td>
<td>Identify risk to be monitored &amp; classify its severity</td>
<td>SOD Summary</td>
<td>Identify the threat and business effect</td>
</tr>
<tr>
<td>Rule Building and Validation</td>
<td>Identify the transactions and authorizations necessary for the threat. Build Transaction Code (T-Code) and SOD object rules to discover the threat. Verify rules against known cases or create test cases.</td>
<td>Delivered assumptions and Rule Architect in GRC Access Control</td>
<td>Build and customize business rules to specification to discover the threat conditions in roles and/or user assignments</td>
</tr>
<tr>
<td>Analysis</td>
<td>Run Analytical Reports</td>
<td>GRC Access Control Management View/Risk Analysis reports – system scans</td>
<td>Identify role changes and/or user assignments to resolve issues.</td>
</tr>
<tr>
<td></td>
<td>Size exceptions</td>
<td>Role reports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confirm rules are working</td>
<td>User reports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modify rules, if necessary</td>
<td>Variants</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Run Management reports</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Analyze roles and users after roles are changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remediation</td>
<td>Determine alternatives to eliminate issues in roles.</td>
<td>Firefighter ID’s to take on infrequent functions like closing periods in conflicts.</td>
<td>Get approval for role modifications to avoid risks inherent in roles &amp; composites.</td>
</tr>
<tr>
<td></td>
<td>Present analysis to respective BPOs</td>
<td>Use of Risk Analysis and Management View reports and Remediation analysis.</td>
<td>Get approval for user changes to avoid risks</td>
</tr>
<tr>
<td></td>
<td>Document corrective actions</td>
<td>Simulation for exclusions and composite utility report.</td>
<td>Determine conditions which cannot be corrected by role or user assignment changes.</td>
</tr>
<tr>
<td></td>
<td>Modify/create roles or user assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mitigation</td>
<td>Design alternative controls to mitigate the risk.</td>
<td>Association of risks and corresponding access controls.</td>
<td>Document controls and personnel responsible for monitoring the risks and assigning alternative controls to user and role</td>
</tr>
<tr>
<td></td>
<td>Educate Management and get approval</td>
<td>Alerts for mitigating controls.</td>
<td></td>
</tr>
<tr>
<td>Phase</td>
<td>Steps</td>
<td>Reference Documents / Tools</td>
<td>Objectives</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Document mitigating controls and monitor.</td>
<td></td>
<td></td>
<td>SOD issues.</td>
</tr>
<tr>
<td>Continuous Compliance</td>
<td>Complete simulation to monitor changes when requests are made for new roles, user assignments or changes.</td>
<td>Simulation capabilities in GRC Access Control</td>
<td>Maintain Continuous Controls Compliance and identify new risks on a proactive basis.</td>
</tr>
</tbody>
</table>
Policies and Standards

Sample Policy

The following is meant to serve as an example and should be revised to fit the client’s control culture. High-level management should issue a policy to provide guidance to the personnel developing rules to monitor risks in the IT system. This can also send a signal to employees that management supports security best practices.

Business Process Owners, Business Process Analysts, and Security personnel must work in a collaborative manner to identify segregation-of-Duties issues and excessive access. This will enable a company to manage risks by implementing corrective measures to eliminate or detect exceptions. The following are general areas of conflict that must be addressed in order to maintain effective internal controls over the business process. These controls will protect the integrity, accuracy and availability of business system information.

- Maintenance of general accounting periods, charts of accounts, and other general infrastructure changes must be segregated from posting, changing, and adjusting capabilities for financial transactions.
- Master data should be segregated from business transactions and vendor/supplier additions and maintenance should be segregated from financial transactions.
- The receipt and maintenance of inventory goods or services must be segregated from order and invoicing activities.
- Banking transactions and changes must be segregated from payment, vendor and posting activities.
- Reconciling and releasing transactions in a suspense or “blocked” status must be segregated from daily processing and posting activities.
- Order, invoice and payment activities should be segregated or monitored if given to one person.
- Invoice posting must be segregated from goods receipt and payment processing.
- Inventory verification or pricing adjustments should be segregated from counting and stock picking activities.
- Maintenance of contracts and terms must be segregated from payment and billing document changes.
Standard Terms and Definitions

Definitions

The Segregation-of-Duties process brings to light new terms that may be common to security and control personnel, but misunderstood or unknown to others. Here is a list of common ones that should be communicated.

Risk Level – The degree or significance of loss to the company if the condition occurs.

SOD – Segregation-of-Duties risks are opportunities for one individual to control a process from beginning to end without the involvement of others. When an individual exploits the condition, data integrity, productivity loss, and physical losses can result without being detected. For example, one person may be able to set up a vendor and process payments, or manipulate sales and customer invoices to conceal kickbacks.

Risks – The opportunity for physical loss, fraud, process disruption, or productivity losses that occur when individuals exploit the condition.

Preventative Controls – Proactive methods used to prevent the occurrence of the risk. For example: Separating duties between organizations and people so two people have to be involved for the fraud to occur. Another example is the regular backup of data to be able to restore critical data when destroyed.

Detective Controls – Methods used to detect the occurrence of bad events after-the-fact. For example: Reviewing key transactions completed by an individual who has the access to set up a vendor and process payments. Another example would be logging changes and reviewing for unusual or unauthorized changes.

Remediation – Actions taken to adjust security access to eliminate the opportunity for risks to occur.

Mitigation – Actions taken to monitor activities when business conditions require personnel to have the opportunity to exploit weaknesses. In these cases, detective controls will be put in place where preventative security controls are too restrictive to business operations.

Monitors – The personnel assigned to execute the alternative controls designed in the Mitigation phase.

Acronyms

PFCG  Profile Generator in SAP used for Role generation and maintenance
BPO  Business Process Owner
BPA  Business Process Analyst
SOD  Segregation of Duties
RTA  Real Time Access – GRC Access Control code loaded to monitored systems
Risk Recognition

Audit and business personnel will from time to time identify undesirable conditions that could allow fraud or significant errors to occur and go undetected across processes (SOD conditions). Rules can be established to monitor security access to make sure these conditions are not permitted without management approval. The objective of this phase is to clarify the business risk associated with the undesirable condition. The principal participants in this phase are the BPO, audit and security personnel. The following are the steps to follow:

Meeting with Business Process Owner

1. The business risk is documented by the BPO.
2. The risk statement should clearly state the actions and the negative results that will occur if the undesired access is exploited.
   a. Example: Create a fictitious vendor and submit invoices for payment.
   b. Example: Adjust orders and receipts to conceal inventory variances
3. From the risk statement, reference similar items in the supplied information:
   a. The Actions list gives the description and corresponding Actions involved in the conflict.
   b. The Security Administrator can review similar risks by reviewing the group risk descriptions.
   c. The object data contains the objects and field values checked for each of the Actions.
4. Meet with the BPO to review the risk and risk level. The discussion and/or simulation of the actual conflict should help achieve the following:
   a. Common understanding between Business, Audit and Security of the access conditions to be avoided.
   b. The severity of the risk assigned by the BPO (High, Medium, and Low per Risk Definitions section).
   c. Document decisions in the SOD resolution document (Appendix II).

Risk Level Rating Criteria

Once the risks are understood, the Business Owner should assess the severity of the risk to the organization if exploited. However, in the absence of common guidelines within the company, here is a sample criterion that can be used or revised by the client. The important aspect is that there is a standard that can be used regardless of individual personal opinions.

High - Physical or monetary loss or system wide disruption can result, such as fraud, system failure, or asset loss.

Medium – Data integrity or manipulation or multiple system disruption can occur, such as master data overwritten, bypassing business approvals, or disruption of multiple business process areas.

Low – Productivity losses or system failures affecting a single unit or operation can result, such as misstatement of internal project costs or system outage for one plant or location.

Documentation & Communication

1. Risk approved for adoption or development by the Business Process Owner.
2. The SOD rule keeper should approve the technical elements of the rule to discover the risk conditions.
3. Discuss any process controls in related areas that might affect the business risk(s).
4. Make sure the risks apply to the organization, i.e. does the organization process rebates? Business personnel should be able to identify those risks that don’t apply.
5. Document the control objective of why this risk should be prevented. Examples of possible control objectives include the following:
   a. Asset Protection
   b. Fraud Prevention
   c. Ensure payments are for legitimate products and services
d. Ensure applicable laws, codes and regulations are adhered to

6. Facilitate the discussion with one of the business owners to go through the risk summary for one group like finance or procurement or conduct a role play with the security personnel to make sure all the information necessary to build the rule to discover the risk will be obtained in the meeting with the business owner.

Rule Building and Validation

After the business risk is clarified and classified, Security and the BPA collaborate to establish the technical rules to monitor the risk. SAP provides a list of SOD risks that have been accumulated from customers, auditors and our own experience. The risks have been validated and tested using standard actions, objects and values. The assumptions used to build these rules should be reviewed to determine their applicability to each client.

Rule Assumptions

Standard action combinations contained in each of the conflicting functions for risks are defined in Rule Architect. The pairs and sometimes three-actions-combinations have been grouped into risk groups. This cuts down the number of issues the business has to worry about and provides a way to check for all combinations. For example, a risk like creating a fictitious vendor and initiating a payment contains the transactions for the conflicting functions: vendor maintenance and A/P payments.

In addition, SOD permission rules contain checks for authorization objects and values for some or all of the actions contained in the conflicting functions. Object level checking is necessary to eliminate false positives and report valid issues. For example, if a person has access to a vendor transaction and a payment transaction, but only has the ability to view the payment information, that person may be reported with a potential risk. However, this is a false positive, as SOD risks are defined as authorizations for create, change, and clearing activities. As these activities are checked in the SOD object level rules, a user who could maintain vendor master data but only view payment details would not be reported in the analysis at object level.

Functions in Rule Architect

The actions used for each of the conflicting functions listed in the risk summary are shown in Rule Architect, under Functions. Functions are maintained to enable or disable certain actions and are the primary components of the risks. The client should review the default list of actions to determine their applicability to their environment. It is recommended that actions which are not active in the production environment but could be at some future date be left in the functions. This allows anticipating SOD issues via simulation capabilities. If the rules do not contain these actions, issues will not be discovered in the role or user analysis.

Object and Value Assumptions

The SOD object level checks for risks enable you to zero in on real issues by checking for activities, account values, order types, etc. which are relevant to the risks. The following are the assumptions:

Account Type (F_BKPF_KOA) checks include the standard SAP default values (A=Asset, D=Customers, K=Vendors, M=Materials, S=General Ledger) and are included based on the SOD function / risk statement. For example, if one SOD function is Process Vendor Invoices, the account type in the object level rule will be K for any transactions containing the object.

Material Views (M_MATE_STA): Delivered rules check for access to create or update basic, accounting, or costing views of the material [K, G or B] Goods Receipts (M_MSEG_BWE): Checking for Movement Types 101 – 106 & 122

Maintain Purchase Orders (M_BEST_BSA): Checking for Purchase Order type EC, FO or NB

Delivery Processing (M_MSEG_BWA): Checking for Movement Types 601 – 602 for VL* transactions [Note: This object is not usually updated in SU24 for the delivery processing transactions. However, a trace determined that this is required for someone to process a goods issue via delivery processing. This activity makes delivery processing an SOD function]

PO Approval – Release Codes / Groups are not checked. If a user has ME28 or ME29N they will be reported as being able to Release POs. If only PO Approval above a certain level is desired, add the appropriate release code and/or group to the object values (M_EINK_FRG)
Sales order document types are not checked. If certain order types are not considered critical, the non-critical order types should be ranged out of the rules (V_VBAK_AAT).

Activities include records that are 01, 02, 05, 06, 77, etc. (activities that allow update access) and disable records where the ACTVT equals 03, 04, 08 (activities which provide only display access).

**HR Object Data**

Only Payroll transactions for US related Payroll are included in the standard rule set. If Payroll is processed for other countries, the country specific transactions should be added to the SOD Rules.

**PA Master Data Infotypes (P_ORIGIN)**

- 0008 Basic Pay
- 0009 Bank Details

**Benefit Processing Infotypes (P_ORIGIN)**

- 0167 Health Plans
- 0168 Insurance Plans
- 0169 Savings Plans
- 0170 Flexible Spending Accounts
- 0171 General Benefits Info
- 0377 Miscellaneous Plans

**HR Configuration Infotypes (P_ORIGIN)**

- 0001 Organizational Assignment
- 0002 Personal Data
- 0003 Payroll Status

**Approve Time Infotypes (P_ORIGIN)**

- 2001 Absences/Attendances
- 2002 Attendances
## Naming Conventions for Business Processes

Each risk can be assigned to a Business Process which is used to provide valuable reporting capability.

<table>
<thead>
<tr>
<th>Business Process ID</th>
<th>Business Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP00</td>
<td>APO</td>
</tr>
<tr>
<td>BS00</td>
<td>Basis &amp; Security</td>
</tr>
<tr>
<td>CA00</td>
<td>Cross Application</td>
</tr>
<tr>
<td>CR00</td>
<td>CRM</td>
</tr>
<tr>
<td>EC00</td>
<td>Consolidation</td>
</tr>
<tr>
<td>FI00</td>
<td>Finance</td>
</tr>
<tr>
<td>HR00</td>
<td>Human Resources &amp; Payroll</td>
</tr>
<tr>
<td>MM00</td>
<td>Material Management/Production Planning/Quality Management</td>
</tr>
<tr>
<td>PM</td>
<td>Plant Maintenance</td>
</tr>
<tr>
<td>PR00</td>
<td>Procure to Pay</td>
</tr>
<tr>
<td>SD00</td>
<td>Order to Cash</td>
</tr>
<tr>
<td>SR00</td>
<td>EBP and SRM</td>
</tr>
</tbody>
</table>
Naming Conventions for SOD Risk Groups

The purpose of the Risk ID is to group multiple combinations of undesired activity into common risk groups. Business personnel can focus on the risk rather than the technical details. The SOD ID is 9 characters in length, and positions 5 to 0 are reserved for GRC Access Control rule sequencing. The naming convention follows for SOD Groups, Rule Building and Backup files:

<table>
<thead>
<tr>
<th>Business Areas -- Position 1</th>
<th>Number or Business Area indicator - Position 2</th>
<th>Sequential number Positions 3-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>A = APO</td>
<td>0 to 9</td>
<td>01 to 99</td>
</tr>
<tr>
<td>B = Basis and Security</td>
<td>0 to 9</td>
<td>01 to 99</td>
</tr>
<tr>
<td>D = CRM</td>
<td>0 to 9</td>
<td>01 to 99</td>
</tr>
<tr>
<td>E = EBP / SRM</td>
<td>0 to 9</td>
<td>01 to 99</td>
</tr>
<tr>
<td>F = Finance</td>
<td>0 to 9</td>
<td>01 to 99</td>
</tr>
<tr>
<td>H = Human Resources &amp; Payroll</td>
<td>0 to 9</td>
<td>01 to 99</td>
</tr>
<tr>
<td>M = MM / PP / QM</td>
<td>0 to 9</td>
<td>01 to 99</td>
</tr>
<tr>
<td>P = Procurement / AP</td>
<td>0 to 9</td>
<td>01 to 99</td>
</tr>
<tr>
<td>S = Sales / AR</td>
<td>0 to 9</td>
<td>01 to 99</td>
</tr>
<tr>
<td>A, B, D, E, F, H, M, P, S</td>
<td>Z = client developed groups or rules</td>
<td>01 to 99</td>
</tr>
<tr>
<td>A, B, D, E, F, H, M, P, S</td>
<td>Z = client developed groups or rules</td>
<td>01 to 99</td>
</tr>
</tbody>
</table>
**Naming Conventions for SOD Functions**

Transactions (and associated object data) can be defined for functions. Naming conventions for delivered functions are shown below:

<table>
<thead>
<tr>
<th>Function ID</th>
<th>Function Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AO</td>
<td>APO</td>
</tr>
<tr>
<td>AP</td>
<td>Accounts Payable</td>
</tr>
<tr>
<td>AR</td>
<td>Accounts Receivable</td>
</tr>
<tr>
<td>BS</td>
<td>Basis &amp; Security</td>
</tr>
<tr>
<td>CA</td>
<td>Cross Application</td>
</tr>
<tr>
<td>CC</td>
<td>Cost Center Accounting</td>
</tr>
<tr>
<td>CR</td>
<td>CRM</td>
</tr>
<tr>
<td>EC</td>
<td>Consolidation</td>
</tr>
<tr>
<td>FA</td>
<td>Fixed Assets</td>
</tr>
<tr>
<td>FI</td>
<td>Finance</td>
</tr>
<tr>
<td>GL</td>
<td>General Ledger</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>MM</td>
<td>Materials Management</td>
</tr>
<tr>
<td>PM</td>
<td>Plant Maintenance</td>
</tr>
<tr>
<td>PP</td>
<td>Production Planning</td>
</tr>
<tr>
<td>PR</td>
<td>Procure to Pay</td>
</tr>
<tr>
<td>PS</td>
<td>Project Systems</td>
</tr>
<tr>
<td>PY</td>
<td>Payroll</td>
</tr>
<tr>
<td>QM</td>
<td>Quality Management</td>
</tr>
<tr>
<td>SD</td>
<td>Order to Cash</td>
</tr>
<tr>
<td>SR</td>
<td>EBP/SRM</td>
</tr>
</tbody>
</table>
# Naming Conventions for Critical Transaction Risk Groups

The purpose of the Risk ID is to group critical transactions into common risk groups. Business personnel can focus on the risk rather than the technical details. The RISK ID is 4 characters in length. The naming convention follows for Critical Transaction Risk Groups.

<table>
<thead>
<tr>
<th>Business Areas -- Position 1-2</th>
<th>Transaction classification -- Position 3-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>AO = APO</td>
<td>AC = Archiving</td>
</tr>
<tr>
<td>BS = Basis</td>
<td>CF = Configuration</td>
</tr>
<tr>
<td>CA = Cross Application</td>
<td>CT = Misc. Critical Transaction</td>
</tr>
<tr>
<td>CR = CRM</td>
<td>MD = Master Data</td>
</tr>
<tr>
<td>FI = Finance</td>
<td>PF = Performance</td>
</tr>
<tr>
<td>HR = Human Resources/Payroll</td>
<td>SC = Security</td>
</tr>
<tr>
<td>MM = Material Management</td>
<td></td>
</tr>
<tr>
<td>PM = Plant Maintenance</td>
<td></td>
</tr>
<tr>
<td>PP = Production Planning</td>
<td></td>
</tr>
<tr>
<td>PR = Procurement/AP</td>
<td></td>
</tr>
<tr>
<td>PS = Project Systems</td>
<td></td>
</tr>
<tr>
<td>SD = Sales/AR</td>
<td></td>
</tr>
</tbody>
</table>
Customizing Rules

The assumptions should be reviewed to make sure the values are valid for your installation of the business system(s). In order to accomplish this, a collaborative effort with the Business Process Analyst who has an in-depth functional knowledge of the system’s configuration and business processes is required. The BPA is usually in a position to review the assumptions and determine any special revisions that have been made to the business system’s configuration. For example, many times order types have been added to recognize an outside order vs. an internal order. Once identified, appropriate changes can be made to tailor the rules to the each client’s business environment.

In addition, there are custom transactions which might have to be added to the action combinations for risks. For example, an upload program is often developed to upload general ledger entries from an external spreadsheet for posting to the GL. These are additional change or create entry points for users that need to be included in the transaction combinations for the relevant risks. Reporting transactions are not relevant but any action that allows for creation or change for any of the relevant areas identified should be reviewed.

The following are the steps recommended to conduct an adequate assessment of the rule assumptions:

Meet with Business Process Analyst

Provide a copy of the assumptions and references to the BPA. If custom transaction and/or objects are involved, make sure to include support personnel in the review to ensure objects are being included or excluded appropriately.

Document any decisions (see SOD Resolution Document -Appendix II) to depict why transactions, objects or values should be enabled or disabled.

Discuss the types of roles and/or users for test cases to validate the rules. If none are available, make some positive and negative test cases by revising existing roles and users in the test client.

Completing Rule Customization Process

After meeting with the BPO and the BPA, the custom transaction and object level changes should be identified. The steps to customize the rules to each organization are covered in the steps below:

Use Rule Architect to make the necessary action and/or permission changes to rules by updating the Function. Both the action and permission level rules should be updated to incorporate the changes in GRC Access Control rules.

Validate the rules by running reports and reviewing the roles and users being reported to make sure rule adjustments are valid for risk discovery.

Validating and Approving Rules

After the rules are built, testing should be conducted to make sure the desired risk conditions are being reported. Use the following steps:

Identify the test roles and user cases for validating the SOD permission rules.

Conduct tests by running reports for the new SOD group and validate that rules are working as intended by running user and role based reports to make sure both positive and negative cases are identified correctly.

As issues are noted and rules are revised, document reasons for changes to rules.

Review the test results with BPAs and BPO and gain their approval.
Analysis

The purpose of the Analysis phase is to provide the BPO and BPA insight to alternatives for correcting or eliminating risks discovered in the following phases. The following steps are completed primarily by the security team to supply decision support information to the BPAs and the BPO. The sequence of the security analysis should be as follows:

- Simple roles
- Composite roles
- Users

Detailed information on remediation steps can be found on the next page.

Confirm Risk Exists

The Security Administrator should display the roles involved and verify through PFCG the presence of the conflicting transaction codes.

Also review the role to determine the presence of objects, fields and values used in the roles that could restrict certain personnel from performing the undesired activities (risks). If all values are available in the roles, different roles could be created to segregate the ability to change or create a specific document as opposed to displaying the document.

Interpreting Reports

There are a variety of reports available to discover and analyze risks. The report types available via the Informer tab in both background and foreground are Executive, Summary and Detail report selections.

- Executive Reports provide a description of the risks and a count of the number of rules which are causing the conflict.
- Summary Reports show the user or role and the corresponding risk group and action conflicts involved. This will make sure no false positives are being investigated prematurely.
- Detail Reports show the source of the conflicts by identifying the specific rule conditions that are being identified by role or user.
- Management View and Risk Analysis reports in the GRC Access Control Informer section are used to provide clients a "scan" of the conflicts for large groups of roles or users. These are excellent reports to size the remediation effort and identify for project management purposes the number of conflicts that need to be resolved. The reports also provide a count of issues which will help identify roles with many conflicts, so further analysis and corrections can be prioritized on those roles with the most issues first.
Remediation

After analysis is underway you will begin to recognize ways to correct conflicts and eliminate issues. Usually the number of violations will be very high because many people have accumulated access and the tracking of changes has not been possible without a software product. The following describes the recommended approach to remediation.

- Resolve the issues in single roles
- Resolve the issues in composite roles
- Resolve user issues

Perform the above tasks in order and try to complete each task before moving to the next. Resolving single role issues will eliminate conflicts in composite roles. Resolving conflicts in composite roles will eliminate user issues. Once both of these tasks have been completed and the changed roles have been moved into Production, begin the User analysis.

Single Role or Composite Role Issue Resolution

Run Risk Analysis for a single role. For selection criteria, enter the first part of the role name for each functional area.

Report Analysis

The first step is to run the Management View/Risk Analysis reports for a selected area like Finance roles, Sales, HR etc. Review the role report for the following:

1. Review the summary report and go to the roles that involve the most users and conflicts.
2. If the conflicts indicate conflicting functions between payments and posting or invoicing functions, the lack of limits defined by KOART, Account Type, are usually a major factor. The detail report can be examined to see if multiple values of account type are being listed. This is a good indication the role has an asterisk in the Account type values.
3. If the conflicts indicate functions associated with Vendors, Customer or Material Master Data, then the associated master data change capabilities need to be removed from the role and placed into another role for selected assignment to personnel by the Business Process Owners.
4. Many times it is helpful to run a foreground report of the role being analyzed so you can switch between summary and detail reports and also use the simulation exclusion capabilities to see if removing certain transactions will correct the outstanding conflicts.
5. Should both functions be in the Role?

No
- Identify value reductions that can help like changing activity from create and change to display OR
- Remove the incompatible duties and place them into another role which can be assigned on an individual basis.

Yes
- If there are not enough users to segregate or it does not make good business sense to segregate, identify mitigating controls.
- Assign control to all users who have the role assigned.
- If the situation might change in the future, it is suggested the incompatible capabilities be placed in separate roles. Assignments can then be adjusted at some future date.
Schedule Working Sessions with Business Process Owner

Make appointments with the Business Unit Experts and/or BPOs to review alternatives for eliminating role issues.

Should both functions be in the Job Role?

No

- Both functions can not or should not be performed with the job role. Analyze GRC Access Control report detail results to determine if the appropriate values are loaded.
- Simulate removing transactions to determine if it will eliminate the risks. When the proper “no conflicts” answer is returned, record the exclusions and document on the SOD Resolution Documentation Checklist

Yes

- Is there additional permission level data that can be identified to further restrict the role like changing activities from create and or change to display only?
- Can system controls/configuration be introduced to minimize the risk?
- If there are not enough users to segregate or does not make good business sense to segregate, identify mitigating controls and assign to all users with the Job Composite Role.

User Issue Resolution

Before running reports on users, make sure that all the corrections have been implemented to roles.

After role cleanup is completed, and super user access has been eliminated by FireFighter, run Risk Analysis report and create reports for each Risk Group Area (Finance, Procure to Pay, etc.) or user groups for distribution to the appropriate business personnel, and review the following:

Should the user perform both functions?

No

- Can one or more roles be removed to remove the access?
- If the user shouldn’t be able to perform both functions based on the role assignment, analyze GRC Access Control Report detail results to determine if the appropriate values are loaded.
- Can additional data be identified to further restrict GRC Access Control Rules?
- Does a role require changes?

Yes

- Can additional object level data be identified to further restrict the role? (Ex., Department personnel should create Purchase Orders but only Plant to Plant Stock Transfers, not to vendors – Role values can be restricted to only Inter-Company order types.)
- Can system controls/configuration be introduced to minimize the risk?
- Identify mitigating control and assign to the user.
Remediation Approval and Documentation

Once the analysis phase is completed, the BPAs and BPOs evaluate the alternatives for resolution. The following are the steps to arrive at an action plan for eliminating the risks.

Meet with the Business Process Analysts

The meeting should confirm the rules in GRC Access Control identify the risks and exceptions correctly. Alternatives for eliminating the conflict should be discussed.

If the risk condition for the role or user cannot be eliminated, proceed to the Mitigation Phase.

Documentation and Communication

The Security Administrator documents the steps to complete remediation in the SOD Resolution Document (Appendix II) for alternatives and changes, which apply to the issue. (i.e. risk statement, classification, SOD rule adjustments, role adjustments, etc.)

Obtain approvals from the BPO of any adjustments to correct the risks and document the reference to them in the SOD Resolution Document. (Appendix II).

The BPO should approve the Implementation Plan and the Security Administrator should document the plan.

If the process gets bogged down because multiple BPOs or Business Area conflicts exist, the arbitrator, Senior Officer, should be notified to arbitrate issues with Business personnel.
Mitigation

If during the remediation phase, the conflicting access is for a legitimate business purpose and either removing or reassigning the access cannot be completed, an alternative control to help manage the risk must be designed, documented and approved. In some cases, existing controls may exist but need to be documented. This phase covers the steps to arrive at an acceptable alternative to manage the risk and document the controls.

Design Controls

The BPO and BPA should collaborate on alternative controls to prevent or detect the risk. Preventative controls are preferred over detective controls because they can be automated and are less dependent upon human intervention. The cost/benefit of developing preventative controls should be carefully analyzed. Developing a custom object that eliminates part of the functionality to a few people may not be the best approach. Since development costs are involved, the potential of the risk should involve significant dollars or transaction volumes. If a preventative control cannot be identified, a detective control for monitoring the risk should be designed.

1. The BPO meets with affected business personnel to discuss and agree on an alternative control or how existing controls are used to monitor the risk.
2. BPA, Security Administrator and the BPO collaborate on alternatives for preventative or detective control alternatives.
3. Security Administrator documents the discussions and decisions in the SOD Resolution Document, Appendix II.

Internal Audit Review (optional)

1. BPA presents alternative controls and reviews with Internal Audit and/or appropriate Business Managers.
2. Internal Audit or Business Manager may review and comment on proposed alternatives.
3. BPA makes any necessary revisions or any adjustment based on comments.

Control Approval and Entry

1. BPO presents to the Senior Officer the following information:
   a. SOD risk statement
   b. Business reasons for access
   c. Remediation alternatives rejected
   d. Alternative control to be implemented
   e. End users or groups affected
   f. Personnel responsible for monitoring
2. Senior Officer notifies BPO(s), Security, Internal audit and BPA of decision and any validity period for the alternative control. The Monitor for the Mitigating control is also designated.
3. The designated mitigation control administrator enters the control and designates monitors in GRC Access Control. The following sequence is required to enter the mitigation control entries:
   a. Mitigation Controls are entered first for the control description, business unit, and approver.
   b. Monitors are entered next to denote the personnel responsible for monitoring the users. Only the personnel designated to enter the user or role assignments need to be system users.
   c. User Mitigation assignments specify the specific risk group and the mitigating reference control that is to be used to manage the risk.
   d. Role Mitigation assignments specify the roles by specific risk group and the mitigating reference control that is to be used to manage the risk.
Implementation

1. If the role is to be mitigated, the BPA or Role Owner enters the role mitigation period and references via an exception report or by using the mitigating controls maintenance function in GRC Access Control.

2. If the user is to be mitigated, the BPO or approver enters the user and corresponding control and monitors from the exception report risk id link or via the Mitigation maintenance facility in GRC Access Control. Users that have mitigated roles assigned must also have an entry in the User Mitigation table.

3. If development resources are required for the mitigating control, the BPO notifies Monitors, Security and appropriate personnel to develop reports or other controls. The action plan and milestones are documented in the SOD Resolution Document, Appendix II.

Mitigating Control Naming Conventions

The following is an example of a naming standard for mitigating control ID’s in GRC Access Control. The important elements are that the people completing the user or role mitigation assignments will readily recognize them and associated with the corresponding risk.

Naming Conventions and Standards

Ref number
Character 1 Business Area designation (A=Accounting, P=Procurement, etc.)
Character 2 User or Role Group Letter (i.e., S=US, E=Europe, A=Asia)
Character 3-10 Sequential Numbers

Description - Must include the report name, and purpose of control.
Business Unit – Location or Area affected.
Management Approval – Mitigation Control Approver’s First and Last Name.
Monitors – Personnel involved in executing the alternative controls defined.
Valid date – Must have a date, evergreen items should be dated no more than three years forward and reviewed again at expiration for renewal.

Mitigation Control Monitoring

After the mitigating control is approved and implemented, the monitor is responsible for using the defined control mechanism to detect exceptions.

Internal auditors or External auditors periodically review or test the control to ensure the control is working to identify exceptions as designed.

Documentation and Communication

1. The BPO or security notifies Senior Officer of SOD issues, which either cannot be corrected, or are in a stalemate status in the process cycle.

2. The SOD resolution document contains the steps of the process and history from risk identification to mitigation.

3. The BPO proposal for Mitigating Controls presented to senior officers should be retained for audit purposes.

4. The mitigation control description monitors and validity periods are documented in mitigating entries for each user and role.
Continuous Compliance
As SOD rules are implemented, new roles and role changes include testing in GRC Access Control to make sure no new SOD risks are introduced. When new requests are made, BPAs and BPOs or approvers should analyze requests using the simulation capability to make sure no new issues appear as a result of the request.

New Role or Change Requests

1. When the BPO or BPA receives a request to add functionality via a transaction code or role, the simulation capability in GRC Access Control should be used to determine if any new risks occur with the request.

2. If the report indicates new and existing issues, use the Simulation Risks only button to determine if the addition is solely responsible for introducing new risks.

3. If issues don’t exist but are created or identified as a result of the request, the BPO or BPA should discuss alternatives with the requesting manager.

New User or User Change Requests

1. Any new user requests are analyzed using GRC Access Control simulation to ensure new SOD risks are not being introduced into the environment with the requested change.

2. If issues are identified, the requesting Manager should be informed by the BPO (Approver) to find an alternative to the request.

3. If an alternative is not available, the Manager and the BPO must design a mitigating control to present for review and approval.

4. If a similar mitigation control exists, the BPO or BPA can enter the user or role mitigation from the detail report showing the risk ID.
Appendix I - Sample Process for Resolution of Segregation-of-Duties Conflicts

Definitions

Segregation of Duties (SOD) - A primary internal control intended to prevent or decrease the risk of errors or irregularities by assigning conflicting duties to different personnel. Categories of duties that should be separated for each of the Company’s business processes are as follows:

Authorization – implied or explicit approval to perform a business transaction or activity.
Custody – activities assigned to personnel to safeguard an asset, including information.
Record keeping – activities to record an action or event in an organization’s records.
Reconciliation – comparisons of recorded balances or volumes to actual results between time intervals to detect differences and take action on any differences.

Mitigating Controls - An alternative control used when it is not possible to segregate duties or established procedures/processes require personnel to have conflicting duties. Mitigating controls can be preventative (e.g. system configuration) or detective (e.g. monitoring transaction activity). Preventative controls are always preferable to detective controls.

Steps for process owners to analyze SOD conditions

1. Review risk statement on the SOD. Consult Finance to understand the risk statement if necessary. Gain an understanding of what the risk is (e.g. is access to create or change certain fields the real issue).

2. Review the current system configuration for the actions to validate the existence of the risk to the organization. For example, actions may limit access to certain views, document types, access types (read-only versus create) that render the risk statement not applicable as users cannot actually perform the conflicting actions. If this is the case, describe such configuration and validate with system security. If this is not the case, continue through the process outlined below.

3. Examine usage reports and processes to see if conflicting duties can be separated. If so, remove the role or find different roles that facilitate this separation or reduce the conflicts. If access cannot be removed or no other roles are applicable, continue through the process outlined below.

4. Work with system security to identify any auth object restriction possibilities. If the authorization objects can be set so that the offending fields cannot be accessed, or the access is restricted to only the values needed for the user to perform their job, this will remove the existence of the risk to the organization.

5. Design other preventative controls via system configuration such as thresholds that when met require higher levels of approval via work flow, or turning off certain transaction code functionality (i.e. MIGO in SAP).

6. If a preventative control can’t be identified, design a method for monitoring the transaction activity. Examples of monitoring controls may include, but are not limited to:
   a. User logs use of transactions with reasons. Reviewer validates log against reports of usage and signs off on the log.
   b. Develop a report that will provide data for reviewers. For instance, there currently is a report in SAP that shows if a user performs a goods receipt for a PO that they created. The report would need to be reviewed on a periodic basis and evidence of this review retained for audit verification purposes.
   c. Use existing reporting functionality to monitor transactions by specified users (i.e. monitor transactions over a certain threshold).
   d. Detailed variance analysis performed by management.
   e. Review of exception reports.

Components of a Mitigating Control

All identified mitigating control documentation will be documented in GRC Access Control tables. The following data is required to be documented:
1. The pair of action codes in conflict and the corresponding GRC Access Control group ID if known. Contact system security if you need assistance in identifying the group ID.

2. A precise description of the mitigating control including the evidence to prove that the mitigating control is being performed and who performs the mitigating control. The level of detail in the documentation should be such that a third party could take the documentation and easily re-perform, observe, or examine the mitigating control. The evidence of the control performance should be evident in the documentation - i.e. a report that is initialed and maintained, an approval form, etc. Clients will be audited against the description both by Internal Audit and external auditors, so the documentation needs to be at an activity level detail and as precise as possible.

3. The name of the manager who is responsible for the mitigating control. This should be the data owner and may or may not be the reviewer for monitoring controls. It is the person that will be contacted if the control is selected for audit procedures. The person responsible for performing the mitigating control should be 1) familiar with the process/procedure being mitigated, 2) independent of the process being mitigated, and 3) should not have the segregation-of-duties conflict that is being mitigated. If a mitigating control owner changes jobs or roles and will no longer be the responsible party for the mitigating control, the mitigating control owner is responsible for communicating such change to the business process owner so that a replacement can be identified and documented in GRC Access Control.

4. The name of the role(s) or user(s) that the mitigation applies to.

5. If applicable, the identified mitigating control may be mapped to external controls documentation.

Approval/Recording of Mitigating Controls

All mitigating controls should be submitted to system security who will verify them from a technical standpoint (e.g. auth object settings, transaction traces, etc.). System security will forward the mitigating controls to Finance (or Compliance or Audit) or approval. After approval is obtained, the GRC Access Control tables will be updated by system security.

Monitoring of Mitigating Controls

All mitigating controls will be subject to audit procedures that will be performed both by internal audit and by external auditors.

Maintaining documentation of the performance of the controls and assisting with the audit of the mitigating control is the responsibility of the manager assigned to the mitigating control.

See example of mitigating control documentation below.

Example of mitigating control documentation format in SAP

Risk:

VA01 “Sales Order Processing”
VL01N, VL02N “Change Outbound Delivery”

The risk here is that an employee could fraudulently add quantities to an order and a delivery and take possession of the items him/herself or create fictitious revenues by delivering unordered materials to customers.

Proposed treatment for t-code:

Document a mitigating control.
Mitigating Controls:

An employee could fraudulently add items to the sales order and/or delivery and issue goods to customer to create fictitious revenues.

If the additional goods were shipped to customers to create fictitious revenue, there are detective controls in place that would identify any material variances in the revenue accounts. Detailed reviews of revenue and expense accounts are performed at least quarterly that compare actual results to prior period actuals and budget. In addition, controls are in place to document, investigate, and resolve issues raised by customers that result in payment issues.

Mitigating Control Owner:

John Doe, Finance Manager
Appendix II – SOD Resolution Documentation Checklist

Business Process Owners (BPOs):
<Names>

Security administrator:
<Names>

Business Process Analysts (BPAs):
<Names>

Auditor:
<Names>

SOD group ID:
List the group or groups that have common risks

List the conflicting action(s) below:

SOD Issue:
State the audit risk statement and any revisions from the BPO and what should be changed in GRC Access Control Action rules.

Source Reference:
What is source of issue? I.e. Audit Report, 2/13/07 – excel file server path etc.

Business Process Owner
State the Meeting decisions and reference approvals for the risk statement and classification of the risk…high, medium, low.

Business Process Analyst
Any simulations or steps completed to verify the existence or non-existence of the risk should be documented here.

Internal Audit
Document any reviews with Internal Audit.
SOD Resolution Alternatives
Document the alternatives to correcting the conflict in the roles.

Risk Recognition / Classification Adjustments
Document here the adjustments or restated risk statements and the classification of the risk as high, medium or low designated by the BPO.

Transaction SOD Rule Adjustments
Document here when adding t-codes to the SOD risk test or combining tests for the same risk with several combinations.

SOD Permission Rule Adjustments
Document here object-based rules that need to be added to make sure the risk exists beyond the transaction level test.

Remediation Alternatives (Eliminating Risk)
Document corrections to roles or assignments to personnel to eliminate the conflicts or risks stated in the audit.

Mitigation Alternatives (Alternate Controls)
Document any alternative controls for any risks when the SOD control CAN’T be used and remediation alternatives have been rejected to eliminate the access.

Approved Implementation

Action Plans:
Document the approved actions for adjustments to the role or user assignments to eliminate risks. Document the steps to implement approved alternative controls for mitigating risks.

Impact Analysis:
Document the potential impact for removing or adjusting the access by specifying the estimated number of roles or users that may be affected.

Approved By:  The BPO or Mitigation Control approver
Date Approved:  <mm/dd/yyyy>

Security

Action(s) Taken:  Document the security administrator actions taken.