

User Guide



Compliance Calibrator Version 4.0 for SAP

COPYRIGHT

© Copyright 2006 Virsa Systems, Inc. All rights reserved. Virsa, Virsa Systems, Access Enforcer, Compliance Calibrator, Confident Compliance, Continuous Compliance, Firefighter, Risk Terminator, Role Expert, ComplianceOne, the respective taglines, logos and service marks are trademarks of Virsa Systems, Inc., which may be registered in certain jurisdictions. All other trademarks are owned by their respective owners. Some or all of the information contained herein may be protected by patent(s) or patent(s) pending in United States and/or foreign jurisdictions for Virsa Systems, Inc.

This document is intended to assist business and IT professionals to develop an understanding of Virsa Systems software products and services and is provided for informational purposes only. It is not intended to be used relied upon as documentation or as a product specification. THE INFORMATION AND CONTENT PROVIDED ON THIS DOCUMENT ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. THE CONTENT OF THIS WEB SITE MAY CONTAIN INACCURATE OR TYPOGRAPHICAL ERRORS AND VIRSA SYSTEMS MAY MAKE IMPROVEMENTS OR CHANGES TO THE CONTENT AT ANY TIME.

June 2006

SAP Security Audit and Segregation of Duties

Introduction	1
Segregation of Duties (SoD) Concept	1
Overview	2
Navigation in Compliance Calibrator	2
Using Compliance Calibrator	3
Compliance Calibrator Menus	3
Compliance Calibrator Toolbar	3
Relating All the Compliance Calibrator Features	3
Risk Analysis	4
Rule Architect	4
Mitigation Controls	4
Alerts	4
VIS Reports, Management Report, and Tool Box Reports and Utilities	5
Configuration Options	5

Managing Risks

Introduction	7
Organizing Risks	7
Anatomy of a Rule	8
Identifying False Positives	9
Using Organizational Rules to Eliminate False Positives	10
Rules Library	10
Defining Business Processes	10
Maintaining Business Processes	11
Defining Functions	11
Updating Object Values	12
Maintaining Functions	12
Editing a Function Definition	13
Copying a Function	13
Defining Risks	13
Creating Rules from Risks	13
Maintaining Risks	14
Reviewing Rules at Transaction or Object Level	15
Defining and Maintaining Critical Transactions	16
Defining and Maintaining Critical Roles and Profiles	16
Defining and Maintaining Object Rules	17
Building an SoD Supplementary Table	17
Configuration Options	17
Defining and Maintaining Organizational Rules	18
Using Organizational Rules	18
Creating a Transport Request for Rule Architect Tables	19

Managing Controls

Introduction	21
Mitigation Controls Module Features	21

Mitigation Controls Library	22
Defining and Maintaining Monitors and Approvers	22
Defining and Maintaining Business Units	22
Configuration Options	22
Assigning Approvers to Business Units	23
Defining Mitigation Controls	23
Mitigating Users, Roles, Profiles, and HR Objects	25
Maintaining Mitigation Controls	26
Reviewing Risk and Control Relationships	26
Reviewing Monitor and Control Relationships	26
Reviewing Controls Assigned to Users, Roles, Profiles, and HR Objects	26
Control Reports	26
Maintaining Control Tables Off-Line	27
Creating a Transport Request for Mitigation Control Tables	27

Managing Alerts

Introduction	29
Assigning Alert Monitors	29
Monitoring Conflicting Transaction Alerts	30
Monitoring Critical Transaction Alerts	31
Monitoring Activity Control Alerts	32
Reviewing Cleared Alerts	32

Running Risk Analyses

Introduction	33
Choosing an Analysis Type	33
Configuration Options	34
Combined Analysis	34
HR Object Based Only	34
Choosing an SoD Risk Level	34
Configuration Options	34
Filtering Reports by Risk	35
Filtering Reports by Organizational Rule	35
Choosing a Report Format	35
Configuration Options	36
Choosing a User Type	36
Specifying Exclusions	36
Configuration Options	36
Choosing a Rules Matrix	36
Choosing a System for Analysis	36
Configuration Options	36
Saving and Using Variants	36
Running Risk Analyses in Background Mode	36
Using the Enable Delta Analysis Configuration Option	37
Configuration Options	37

Running Simulations

Introduction	39
Configuration Options	39
Simulating Risks for Users and User Groups	39
Simulating Risks for Roles and Profiles	39

Editing Objects for Simulation	40
Role Assignment through Simulation	40

Risk Analysis Reports

Introduction	43
Reporting Features	43
SoD at Transaction Code Level Reports	43
SoD at Authorization Object Level Reports	44
Assigning Controls to Risks	44
Critical Transactions Reports	46
Critical Roles and Profiles Reports	46
Mitigation Controls Reports	47
Simulation Reports	47
Background Reports	47
Management Reports	48
Analytical Report	49
Invalid Mitigating Controls Report	50

Tool Box Reports and Utilities

Introduction	53
Rule Architect Reports and Utilities	53
Authorization Object by Roles/Profiles Report (not in SoD Tables)	53
Comparing Critical Transaction Matrices	53
Comparing SoD Authorization Objects	53
Optimizer for SoD Data Table	54
Comparing Different SoD Matrices	54
SoD Rule Validation Tool	54
Field Definitions	54
Non Reference Report	55
TCodes by Roles/Profiles Never Executed in a Specific Time Period	55
Field Definitions	56
Maintain ORGUSERS Table	56
Scheduling a Background Job	56
Mitigation Control Reports	57
Where Used List for Mitigating Control Reference Monitor	57
Alerts Module Utilities	58
Activity Monitoring	58
Field Definitions	58
Scheduling a Background Job	59
Risk Analysis Reports	59
User Access Report	59
Maintaining the Critical Objects Table	60
Analysis of Called Transactions in Custom Code	60
Management Report for SoD Remediation	61
Monitor Actual Usage of Conflicting & Critical Transactions	62
Processing Field Definitions	62
Select the Type of Analysis Field Definitions	62
Managements Reports	62
Count Authorizations for Users	63
Field Definitions	63
Count Authorizations in Roles	64

Display Changes to Profiles	64
Security and Controls Policies and Procedures	64
Creating the Security Policy Document	65
Specify the Security Policy Document Text	65
Viewing the Security Policy Document	65
Expired and Expiring Roles for Users	65
Field Definitions	65
Maintenance Utilities	66
Compliance Calibrator Data Maintenance	66
Rule Architect Wizard	66
Overview	66
Preparing the Predefined Rule Architect Data Files	67
Running the Rule Architect Wizard	68
Step One - Check Rule Architect Configuration	68
Step Two - Upload Predefined Virsa Rules	68
Step Three - Assigning transactions	69
Step Four - Assigning Objects	69
Step Five - Generate Transaction Code and Object Rules	70
Upload/Download Compliance Calibrator Tables	70
Download Spool Request by Job Name	71

Appendix A. Configuration Options.....A-1

Introduction	1
Rule Architect Options	1
Rule Architect Activation	1
Mitigation Controls Options	1
Date Range Limit for Mitigating Controls	1
Enable Business Unit Authorization Check for Mitigation	1
Enable User Group Authorization Check for Mitigation	2
Enable Risk Level Authorization Check for Mitigation	2
Enable Role Level Authorization Check for Mitigation	2
Enable HR Object Level Authorization Check for Mitigation	2
Risk Analysis Options	2
Default Type of Report	2
Default Risk Level	2
Default User Type	2
Include Reference User in User Analysis	3
Ignore All Critical Roles/Profiles	3
Set Locked Users	3
Set Expired Users	3
Set Mitigating Control	3
Cross-System ID	3
RFC Destination for Remote Simulation	4
Use SoD Supplementary Analysis	4
Use AND Option in Users & User Groups	4
Risk ID	4
Report Options	4
Display Long Risk Description	4
Show All in Report	4
Show Composite Role in User Analysis	4
Default Report Format	4
Set Default Business View	5

Compliance Calibrator Tables Display Format (Tab/ALV)	5
Customer Specific Header Text	5
Include Role/Profile Mitigating Controls in User Analysis	5
Security & Controls Policies & Procedures	5
Program Options	5
Memory Variable for Batch Size	5
Batch Size for Users	5
Batch Size for Roles	5
Multiple Spool Options	5
Threshold Value for Users Analysis	6
Threshold Value for Role/Profile Analysis	6
Cross-System SoD Analysis	6
System Administrator Lock	6
PFCG Plugin	6
Enable Delta Analysis	7
Custom Utilities	7
Log file location	7
Rule Batch size for New Compliance Calibrator BAPI	7
Appendix B. Not Logic.....	B-9
Introduction	9
SOD rule with one NOT	9
SOD rule with two or more NOT for different Object/Field combinations	9
SOD rule with two or more NOT for same Object/Field combinations	9
Appendix C. Defining RFC Destinations	C-11
Introduction	11
Defining an RFC	11
Appendix D. Using a Non-sequential Range of Values.....	D-1
Introduction	1
Importing a Text File	1
Appendix E. Long Descriptions in Transport Requests.....	E-3
Introduction	3
Adding Long Descriptions to the Transport	3
Appendix F. Post Installation Customization	F-7
Delivery Customizing	7
Installing Virsa Objects	7

1. SAP Security Audit and Segregation of Duties

Introduction

SAP Compliance Calibrator by Virsa Systems is a fully automated SAP Security Audit and Segregation of Duties (SoD) Analysis Tool, designed to identify, analyze and resolve all SoD and audit issues.

Compliance Calibrator helps all key stakeholders in SAP Security to work in a collaborative manner to achieve ongoing SoD and audit compliance at all levels, including User, Role, Profile, and HR Object levels. It empowers SAP Security Administrators, Business Process Owners and Internal Auditors to prepare their SAP systems for an audit. User Administrators can use Compliance Calibrator to identify potential SoD issues before assigning a new Role to a User.

Compliance Calibrator, an ABAP-based tool, runs within SAP and thus eliminates the need for additional hardware, software and manual processes to download and manipulate data. It uses custom tables to store SoD data, provide powerful features and to ensure there is no interference with the existing security processes and procedures. Compliance Calibrator produces SoD Analytical Reports (both Summary and Detail) against Users, User groups, Roles and Profiles. It also provides an option to produce reports on critical transactions, critical authorizations, critical Roles and Profiles.

Compliance Calibrator offers comprehensive risk management functionality and provides powerful and easy to use functionality to document Risk Mitigation Controls.

Compliance Calibrator provides user-friendly summary and drill-down reports, making the identification and resolution of SoDs and audit issues a painless process.

It provides Supplementary SoD Analysis to facilitate advanced SoD analysis. This functionality is useful for clients using User Parameter tables (USR05) or other custom (Z) tables to implement enhanced access restrictions.

The Compliance Calibrator Tool Box provides complementary reports and allows clients to link their own custom reports to help in automating various activities related to SoD analysis.

NOTE: Please refer to SAP Note #861556 for information regarding the installation procedures for SAP Compliance Calibrator by Virsa Systems.

Segregation of Duties (SoD) Concept

SoDs are a primary internal control intended to prevent, or decrease the risk of errors or irregularities, identify problems, and ensure corrective action is taken. This is achieved by assuring no single individual has control over all phases of a business transaction.

There are four general categories of duties:

- Authorization
- Custody
- Record keeping
- Reconciliation

In an ideal system, different employees perform each of these four major functions. In other words, no one employee has control of two or more of these responsibilities. The more negotiable the asset, the greater the need for

proper segregation of duties - especially when dealing with cash, negotiable checks and inventories.

There are business areas where SoDs are extremely important. For example, Cash Handling, because cash is a highly liquid asset. This means it is easy to take money and spend it without leaving a trail of where it went. Any department that accepts funds, has access to accounting records, or has control over any type of asset should be concerned with segregation of duties. Some examples of incompatible duties are:

- Authorizing a transaction, receiving and maintaining custody of the asset that resulted from the transaction.
- Receiving checks (payment on account) and approving write-offs.
- Depositing cash and reconciling bank statements.
- Approving time cards and having custody of pay checks.

SoDs can be quite challenging to achieve in a small operation, as it is not always possible to have enough staff to properly segregate duties. In those cases, management may need to take a more active Role to achieve separation of duties, by checking the work done by others or using other Mitigating Controls.

Compliance Calibrator helps automate all SoD-related activities. For example, defining and monitoring SoD conflicts, proactive prevention of SoD conflicts and the use of Mitigation Controls.

The following sections explain these Compliance Calibrator features in detail.

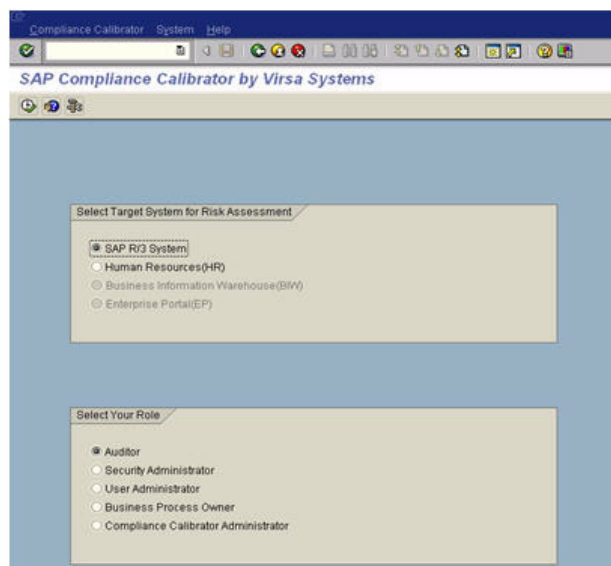
Overview

This manual describes the SAP Compliance Calibrator by Virsa Systems 4.0 features and functionality for versions SAP 4.6b, 4.6c, and higher.

Navigation in Compliance Calibrator

Compliance Calibrator may be accessed via the User Menu or by entering transaction code [/N/VIRSA/ZVRAT].

Figure 1-1: Choosing a module for risk assessment



Perform the following steps.

1. Select the Target System for Risk Analysis.

2. Select a Role
3. Click Execute.

Using Compliance Calibrator

Compliance Calibrator's Risk Analysis Control Panel enables Users to perform all audit-related tasks from one screen. Risk Analysis is performed from the Control Panel. All the other Compliance Calibrator features can be accessed from the toolbar.

Figure 1–2: Compliance Calibrator Menus and Toolbar



Compliance Calibrator Menus

Compliance Calibrator menu - provides access to all the configuration options. It also contains a menu item to run risk analyses in the background.

- **Utilities Menu** - provides access to the Invalid Mitigation Controls Report
- **Custom Utilities menu** - only appears if the Configuration Option Custom Utilities is set to YES.

Compliance Calibrator Toolbar

Execute - This button is used to generate a risk analysis once you have entered all the appropriate values in the Risk Analysis form.

Variants - Clicking this button displays all your saved variants. These can be used to rerun standard risk analysis..

Simulation - Clicking this button displays the simulation screens for running User and Role/Profile simulations.

Rule Architect - Clicking this button displays the Rule Architect..

Mitigation - Clicking this button displays the Mitigation Controls features.

Alerts - Clicking this button displays the Alerts features.

Management Reports - Clicking this button displays the Management report.

Tool Box - Clicking this button displays the Compliance Calibrator Tool Box. The Tool Box contains various reports and utilities..

Help - Clicking this button displays a help screen that provides an overview of running a risk analysis and simulations.

NOTE: The Variants button appears only if you have saved one or more variants.

Relating All the Compliance Calibrator Features

Compliance Calibrator provides the ability to perform several major functions -

- Determine and report if there are any risks associated with a group of transactions or objects and a User, Role, or Profile.
- Determine and report if any risks will be introduced by simulating the addition of transactions, Roles, or Profiles to a User ID. This powerful feature effectively eliminates new risks being introduced to your production environment.
- Easily create, maintain, and manage Risks used to generate Rules.
- Apply Controls to mitigate any Risk associated with a User, Role, or Profile.
- Alert the appropriate monitor when conflicting or critical transactions are used, or a control is assigned to mitigate a risk.
- Alert the appropriate manager when activity monitoring is not performed.

Risk Analysis

When you run a Risk Analysis or a Simulation you generate reports presenting different types of information. You may generate reports presenting risks or conflicts or the use of critical transactions by the User, Role, Profile, or HR Object you included in the analysis.

By generating these reports you can identify the Risk and either remove it or apply a control.

Rule Architect

In order to identify the Risks produced in Risk Analysis reports you need to identify the combinations of SAP transactions and authorization objects that represent conflicts. Compliance Calibrator's Rule Architect provides all the tools you need to define SoDs and Business Processes, and generate the Rules used during Risk Analysis.

In addition to Rules and Business Processes Rule Architect is used to build and maintain tables for Critical Transactions, Critical Roles, and Critical Profiles, as well as other tables.

Mitigation Controls

Once you have run a Risk Analysis and have identified any Risks associated with a User, Role, Profile, or HR Object you may want to limit or monitor the Risk rather than removing the cause.

Mitigation Controls gives you the ability to associate controls with Risks so they may be applied to Users, Roles, Profiles, or HR Objects identified with SoDs through Risk Analysis. You also define monitors and approvers and assign them to specific controls, and create Business Units to help categorize your Mitigation Controls.

Alerts

Alerts are generated for the following reasons -

- A critical transaction was executed
Critical transactions are maintained through the Rule Architect.
- A conflicting transaction was executed
Conflicting transactions are those listed in the SoD transaction level Rules table and are maintained through the Rule Architect.
- A Mitigation Report transaction was not run within the specified time period
These report transactions are a part of a Mitigation Control definition.

Alerts are listed in the Alerts module and can also be emailed to anyone specified in the Alerts Email configuration table.

VIS Reports, Management Report, and Tool Box Reports and Utilities

The two reports listed under the VIS menu provide information on critical transactions at Authorization Object Level.

The Management Report accessible from the Control Panel toolbar displays a snapshot of Risk Statistics in statistical and chart format.

Tool Box Reports and Utilities provide additional administrative and maintenance tools.

Configuration Options

The Configuration Options enable you to set defaults for running Risk Analyses and Report types, various program defaults, and set switches for Mitigation Controls and the Rule Architect.

2. Managing Risks

Introduction

Risks and Rules are defined through the Rule Architect. You can access the Rule Architect by clicking the associated button on the Control Panel toolbar. The Rule Architect screen has the following sections.

- Rule Architect menu - This list provides access to all the features of the Rule Architect. The sections below describe each menu item.
- Work Area - The area to the right of the Rule Architect menu is where the forms appear when you click on a menu item. These are the forms used to build all the features supported by the Rule Architect. The sections below describe the forms for each menu item.

Organizing Risks

A Risk is defined as two or more transactions that, when available to a single user, role, profile, or HR Object create the possibility of error or irregularity. There are thousands of transaction combinations that can be categorized as Risks. Risks can also be defined by different combinations of authorization objects associated with specific transactions.

Another name for combinations of two or more transactions is *functional group*. Individual users, roles, or profiles can access these risks or functional groups in order to perform specific business function.

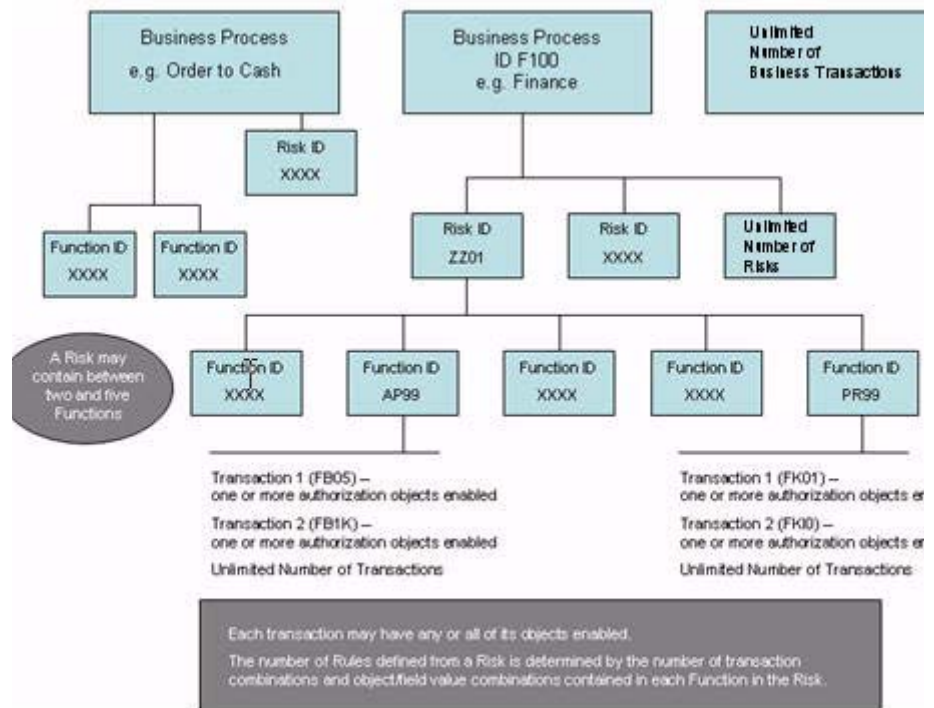
In order to reduce the time and resources needed to manage all combinations Risks can be grouped by Business Processes, ordered by Functions, categorized by Organizational Rules and assigned Risk Levels.

Now we can expand the definition of a Risk by including the combination of two or more Functions in which the combinations of transactions in the two Functions create a Risk. It is from these combinations at transaction level and authorization object level that Rules are created.

Using Compliance Calibrator's Rule Architect, you have the ability to group transactions into Functions and group Functions into Risks. A further level of management control is possible within Compliance Calibrator by creating an overall Business Process and grouping Risks and Functions within it.

The Rule Architect provides all the tools you need to manage risks. The sections below describe the tools and tables located in the Rule Architect.

Figure 2-1: Risk Organization



Anatomy of a Rule

This section uses screen shots to describe the process used to generate Rules at transaction and authorization object levels from Functions and Risks. Refer to the sections below for more information on how to create Functions and Risks.

In this example the Risk ID is ZZZZ. Risk ID ZZZZ is defined with five functions to illustrate how a set of Rules are generated from one Risk. The two Functions contain conflicting transactions. Function AP99 contains a transaction for Posting (FB05) and Function PR99 contains a transaction for Creating a Vendor (FK01).

This first screen shot shows Rule ZZ01001 created at transaction level from Risk ZZ01.

When you generate Rules from Risk ID ZZ01 one transaction level Rule is created and two authorization object level Rules are created. From these two screen shots you can see a transaction level Rule ID is comprised of the four characters from the Risk ID plus a three digit number - ZZ01+001. An authorization object level Rule ID is nine characters - ZZ01+001+01.

Figure 2-2: Transaction Level Rule

Conflicting Transactions	Risk Description	Level	Status
Posting with Clearing (FB05) & Create Vendor (Accounting) (FK01)	ZZ01001:	Medium	Enabled

This second screen shot shows the two Rules created at authorization object level from the same Risk ID ZZ01. Each transaction has only one authorization object enabled, the S_Tcode object and the S_Tcode object has

only one field or value. That is why there are only two authorization object level Rules generated from Risk ZZ01.

Figure 2-3: Authorization Object Level Rules

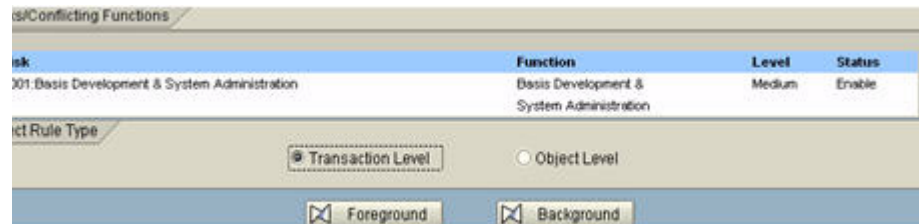
Description	Authorization Object	Field	From	To	Srch Level	St
00101:	S_TCODE : Authorization Check for Transaction Start	Transaction code	PostwithClearing(FB05)		Medium	Er
00101:	S_TCODE : Authorization Check for Transaction Start	Transaction code	CreateVendor(Accounting)(FK01)		Medium	Er

In these next two screen shots there is a second transaction added to each Function. Function ID AP99 now has transactions FB05 and FB1K and Function ID PR99 now has transactions FK01 and FK10. Since there are four combinations between the four transactions, four Rules are generated at transaction level. Since there is one authorization object enabled in each transaction (S_Tcode) and the authorization object has only one field/value, there are eight Rules generated at authorization object level. Note the authorization objects are associated with their respective transactions.

Figure 2-4: Transaction Level Rules

Conflicting Transactions	Risk Description	Level	Status
with Clearing (FB05) & te Vendor (Accounting) (FK01)	ZZ01001:	Medium	Enable
with Clearing (FB05) & te Report (FK00)	ZZ01002:	Medium	Enable
Vendor (FB1K) & te Vendor (Accounting) (FK01)	ZZ01003:	Medium	Enable
Vendor (FB1K) & te Report (FK00)	ZZ01004:	Medium	Enable

Figure 2-5: Authorization Object Level Rules from Enabled Objects



Each time you enable another authorization object additional Rules are generated to cover the additional field or value combinations. If you change the field values of an object any existing Rule built from the object is disabled and a new Rule is added to the Authorization Object Rules table. Using the logical operators OR or NOT you can further calibrate your Rules table.

As you can see the granularity of Rules generated at authorization object level provides the ability to generate very accurate Risk Analysis reports. And that means you can identify and eliminate false positives.

Identifying False Positives

The definition of a false positive is a SoD identified at transaction level for a User, Role, Profile, or HR Object that is eliminated when a Risk Analysis is run at authorization object level.

An example of this is a Risk with conflicting transactions FB05 (Posting) and FK01 (Create Vendor). When you generate Rules from this Risk the transaction FB05 contains the object K_TP_VALU and the ACTVT field value is set to 01 (Create). When you run a Risk Analysis for a User with access to both transactions (FB05 and FK01) a SoD is generated at transaction level.

But if the User's access to FB05 is limited by the ACTVT field value of 03 (Display) running a Risk Analysis for the User at authorization object level eliminates the SoD.

Using Organizational Rules to Eliminate False Positives

Another way to eliminate false positives is using Compliance Calibrator's Organizational Rules. Organizational Rules allows you to filter a Risk Analysis based on Organizational Levels.

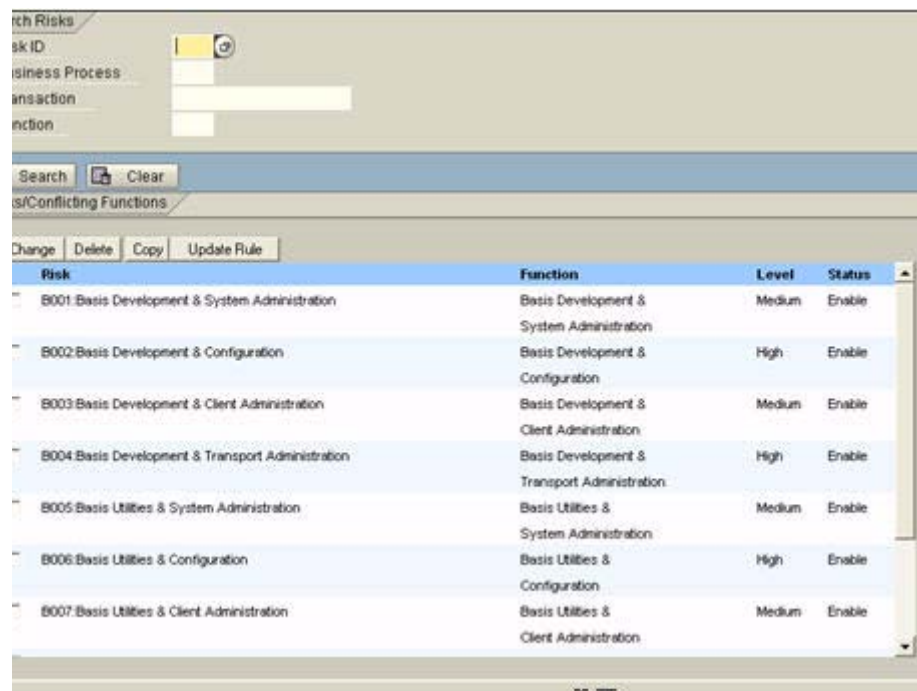
If you run an analysis on a User it may identify a SoD for conflicting transactions such as FB01 (Posting a Payment) and XK01 (Create Vendor). Applying an Organizational Rule to the analysis might remove the SoD.

The SoD is eliminated because the User being analyzed has access to FB01 for one Organizational Level e.g. Company Code (BUKRS) US01, and access to XK01 for different Company Code. By applying an Organizational Rule you have eliminated the false positive.

Rules Library

When you first enter the Rule Architect the Rules Library is displayed. The Rules Library displays a statistical snapshot of all the rules used by Compliance Calibrator, sorted by Business Process.

Figure 2–6: Figure 1 7, Rules Library



Risk	Function	Level	Status
B001: Basis Development & System Administration	Basis Development & System Administration	Medium	Enable
B002: Basis Development & Configuration	Basis Development & Configuration	High	Enable
B003: Basis Development & Client Administration	Basis Development & Client Administration	Medium	Enable
B004: Basis Development & Transport Administration	Basis Development & Transport Administration	High	Enable
B005: Basis Utilities & System Administration	Basis Utilities & System Administration	Medium	Enable
B006: Basis Utilities & Configuration	Basis Utilities & Configuration	High	Enable
B007: Basis Utilities & Client Administration	Basis Utilities & Client Administration	Medium	Enable

Defining Business Processes

Business Processes are created in order to group related Functions and Risks.

When you define Risks and Functions using Rule Architect you must assign them to a Business Process. The first thing you need to do is define your Business Processes.

When you define a Business Process you create a four character Business Process ID and provide a description.

To define a Business Process click the arrow to the left of Business Processes in the Rule Architect menu and then click Create. The Business Process Creation form is displayed in the work area.





When you define a Business Process it is created as an empty group. As you define Functions and Risks you'll associate them to one or more Business Processes.

Maintaining Business Processes

Once a Business Process is defined you can change its description or delete it. If you delete a Business Process none of the associated Risks or Functions is deleted.

To see the list of your Business Processes click the arrow to the left of Business Processes in the Rule Architect menu and then click Display/Change. To edit, display, or delete a Business Process click on it to select it and click the appropriate action button below the form. You can edit or display only one Business Process at a time.

Figure 2-7: Displaying a List of Business Processes

Critical Profiles			
Profile	Risk Description	Risk Level	Status
AP_ALL	All Authorizations For The SAP System	High	 Enable
AP_NEW	All Authorizations For Newly Created Objects	High	 Enable
_A_ADMIN	Basis Operator	High	 Enable
_A_CUSTOMIZ	All Customizing Access - Complete IMG Access	High	 Enable

Defining Functions

A Function is a grouping of transactions. The transactions you group within a Function are all related to performing a specific business function and as a functional group do not present a risk. To define a Function, click the arrow to the left of Functions in the Rule Architect menu and then click Create.

When you define a Function you take the following actions:

1. Create a Function ID
2. Every Function has a unique four character Function ID
3. Provide a description to help define the Function.
4. Add transactions to the Function
You can assign as many transactions to a Function as you like. It is recommended you do not include more than 30 transactions in any one Function. Clicking in the Transaction Code field and then clicking the search button displays a list of available transactions. Once you choose a transaction from the list its description is displayed in the Description field. You can also add your own description in the Custom Description field.
5. Set the Status of the added transaction.
The Status field is used to Enable or Disable the transaction being added to the Function. A transaction with an Enabled Status is included when updating the Rules tables.

CAUTION: If you are using SAP Compliance Calibrator by Virsa Systems version 4.6b, please skip to step 7. SAP Compliance Calibrator by Virsa Systems version 4.6b does not support Coupled Transactions.

6. Check for Coupled Transactions.
Click the Coupled Transactions button to check if there are any parameter or z-transactions coupled to the ones you entered. If you want to include any of the listed transactions select them and click Enter.

NOTE: When you click Coupled Transactions, Compliance Calibrator checks for three conditions. If an SAP transaction assigned to the Function is called by a Custom transaction, the Custom transaction is included in the Coupled Transactions list."If a Custom transaction assigned to the Function is calling any SAP transactions or Custom transactions, the called transactions are included in the Coupled Transactions list." The transaction assigned to the Function is checked in SU24 for any original tcode (parameter transactions). Parameter transactions are also included in the Coupled Transactions list.

7. Assign one or more Business Processes to the Function
Click the checkbox to the right of each Business Process.
8. Optionally change any Object Values
When you click the Save button you are asked if you want to update any Object Values associated with the transactions you've added to the function. Click Yes to display the Object Values list.

Updating Object Values

The Object Values form has a Business View and a Technical View. The Business View is displayed as a tree hierarchy. You can update Object Values through the Business View.

Locate the Object you want to update and click the **Pencil** icon to display the Object Values change form. You can also toggle the status of an object by clicking the **Match** icon to the far right of the object. Toggling an object's status either enables or disables the object. Enabled objects and their field or values are used to generate Rules at authorization object level.

Figure 2–8: Viewing a List of Objects Within a Function



Maintaining Functions

You can change any part of a Function definition except its ID. To maintain a Function click the arrow to the left of Functions in the Rule Architect menu and then click **Display/Change**.

You can search for a specific Function by entering the Function ID. Select the Function from the list and then click **Change** to display the Function attributes.

WARNING!: If you Delete a Function all the Rules created from the Function are also deleted.

Figure 2–9: Displaying a List of Functions



The screenshot shows the 'List of Functions' window in SAP. At the top, there are input fields for 'Function', 'Business Process', and 'Transaction', each with a search icon. Below these is a 'Search' button and a 'Clear' button. The main area is a table with two columns: 'Function ID' and 'Description'.

Function ID	Description
AP01	AP Payments
AP02	Process Vendor Invoices
AP03	Release Blocked Invoices
AP04	Change Vendor Document
AP05	Vendor Payment Release

Editing a Function Definition

Once you have chosen a Function to edit from the list, the same form used to define the Function is displayed. Use the **Plus** and **Minus** icons to add or delete transactions from the function. After making any changes you'll be able to update object values once you click the **Save** button.

Copying a Function

You may want to make changes to the Object Values contained in the transactions in a Function and then generate additional Rules based on the new object field or values. You can copy a Function, make your changes and then update the Rules tables.

Defining Risks

Risks are defined by grouping Functions containing conflicting transactions. To define a Risk click the arrow to the left of Risks in the Rule Architect menu and then click Create.

When you define a Risk you take the following actions:

1. Create the Risk ID
This is a four character ID.
2. Set the Risk Level for the Risk.
The Risk Level is used when running a Risk Analysis. You can limit the analysis to a particular Risk Level.
3. Set the Status of the Risk to Enable or Disable the Risk.
The Risk Status determines whether or not the Risk is included during Risk Analysis.
4. Create a short and detailed Risk Description.
5. Enter a Control Objective
The Control Objective is a short statement describing the grounds for a Risk.
6. Assign a Business Process to the Risk.
7. Assign Functions to the Risk.
You can assign between two and five Functions to a single Risk.

Creating Rules from Risks

When you click Save after defining a Risk you're asked if you want to update the Rules from all the combinations of transactions contained within the Functions assigned to the Risk. If you want to update the Rules table the following form is displayed.

Figure 2–10: Creating Rules from Risks

Risk	Function	Level	Status
001 Basis Development & System Administration	Basis Development & System Administration	Medium	Enable

Select Rule Type

☒ Transaction Level ☐ Object Level

Foreground Background

You can create rules based on the transaction combinations or create rules at the object level. If you have many transactions within the Functions assigned to the Risk you should update the Rules table in the background.

CAUTION: If you generate any new Rules after running a Risk Analysis with the Configuration Option Enable Delta Analysis set to YES you must force a full scan in order to re-analyze all Users, Roles, and Profiles stored in the tables maintained by the option. To do this, check Force Full Scan when you run a background analysis.

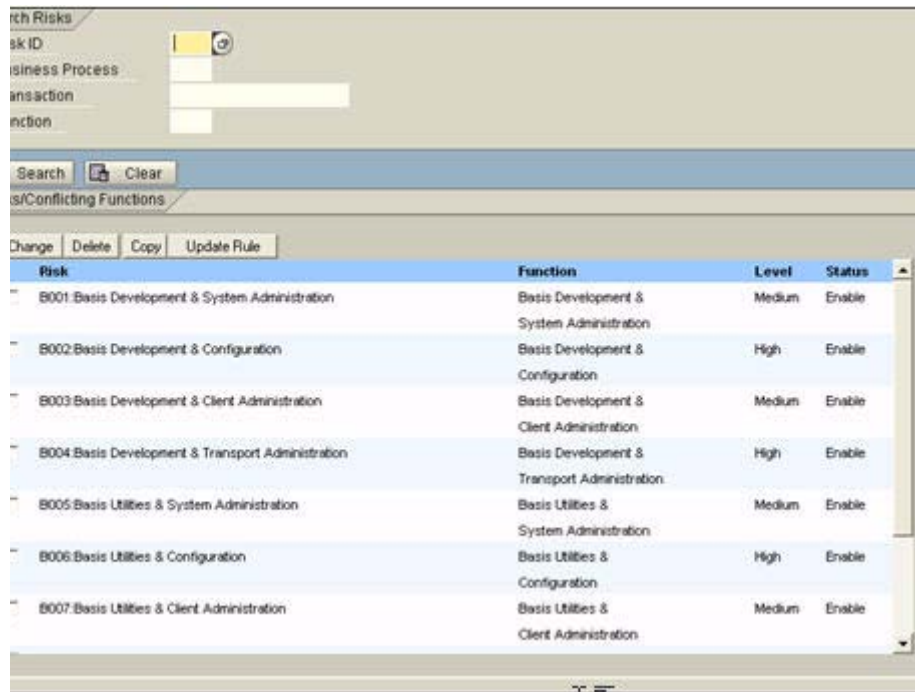
Maintaining Risks

Risks can be redefined by adding or removing Functions, changing descriptions, or assigning it to a different Business Process. Once you have located the Risk you want to change click the Change button to display the same form used to define Risks.

To maintain a Risk click the arrow to the left of Risks in the Rule Architect menu and then click Display or Change.

NOTE: Your ability to maintain Functions and Risks or to search and display Risks is determined by the Compliance Calibrator Role your User ID is assigned. Refer to Compliance Calibrator Security Authorizations Guide for more information.

Figure 2–11: Displaying a List of Risks



Risk	Function	Level	Status
B001: Basis Development & System Administration	Basis Development & System Administration	Medium	Enable
B002: Basis Development & Configuration	Basis Development & Configuration	High	Enable
B003: Basis Development & Client Administration	Basis Development & Client Administration	Medium	Enable
B004: Basis Development & Transport Administration	Basis Development & Transport Administration	High	Enable
B005: Basis Utilities & System Administration	Basis Utilities & System Administration	Medium	Enable
B006: Basis Utilities & Configuration	Basis Utilities & Configuration	High	Enable
B007: Basis Utilities & Client Administration	Basis Utilities & Client Administration	Medium	Enable

There are four actions you can take once you locate a Risk:

1. **Change** - Clicking this button displays the same form used to define a Risk.
2. **Delete** - Once you place a checkmark next to one or more Risks you can click this button to delete the Risks.
CAUTION: Deleting a Risk also deletes all the transaction and object level Rules created from the Risk.
3. **Copy** - You can also copy a Risk and then make changes to the copy. You can only Save a copy of a Risk if it has a unique Risk ID and unique combination of Functions.
4. **Update Rule** - If you have created a Risk and did not create Rules from it you can click this button to display the Update Rules form.

CAUTION: If you generate any new Rules after running a Risk Analysis with the Configuration Option Enable Delta Analysis set to YES you must force a full scan in order to re-analyze all Users, Roles, and Profiles stored in the tables maintained by the option. To do this, check Force Full Scan when you run a background analysis.

Reviewing Rules at Transaction or Object Level

You can view the Rules created from your defined Risks at transaction level or object level. You cannot make changes to Rules in either view. If you want to update a Rule you must make changes to the Functions and Risks used to create the transaction level and authorization level Rules and then update the Rules tables.

Rules are created from the Risks you define and Risks are a collection of Functions. Functions are a collection of transactions and each transaction contains objects with certain field or values. Once you redefine a Function by adding or removing transactions, enabling or disabling objects, or changing field or values of an object you can update the Rules generated from the Risks associated with the redefined Function.

To display transaction level Rules click the arrow to the left of Rules in the Rule Architect menu and then click Conflicting Transactions. To display authorization object level rules click Auth. Object Rules.

When you list Rules you can filter your search by Business Process, Risk ID, Rule ID, Risk Level, and Rule Status. The first three fields accept wildcards. If you are searching for object level Rules you can also filter the search by authorization object and field name. These filters also accept wildcards.

Once your search is complete you can view the list of Rules in Business View or Technical View.

Defining and Maintaining Critical Transactions

If you want to run a Risk Analysis to determine what Critical Transactions are available for a User, Role, Profile, or HR Object you must first identify all your critical transactions.

You can define Critical Transactions through the Rule Architect interface or you can create them with a spreadsheet program and then upload the data to Compliance Calibrator's Critical Transactions table. You can use the New Entries button to add records to the table.

If you upload the data from a spreadsheet file it must be in the same form as shown below, with five columns of information.

The Risk ID in the Critical Transactions table is not associated with Risk IDs assigned when you define Risks. Critical Transaction Risk IDs are used only when running a Risk Analysis to generate a Critical Transactions report.

You can use the Risk IDs defined in the table to create Critical Transaction groups that can be used when generating a Critical Transaction Risk Analysis report.

NOTE: If you set the status of a Critical Transaction to Disable the transaction is not included in any Risk Analysis and does not generate an Alert if the transaction is executed.





Defining and Maintaining Critical Roles and Profiles

Critical Roles and Critical Profiles are used to generate specific Risk Analysis reports.

You can define Critical Roles and Profiles through the Rule Architect interface or you can create them with a spreadsheet program and then upload the data into Compliance Calibrator. You can use the New Entries button to add records to the table.

If you upload the data from a spreadsheet file it must be in the same form as shown below, with four columns of information.

Figure 2-12: Critical Roles and Profiles

Critical Profiles			
Profile	Risk Description	Risk Level	Status
AP_ALL	All Authorizations For The SAP System	High	 Enable
AP_NEW	All Authorizations For Newly Created Objects	High	 Enable
_A_ADMIN	Basis Operator	High	 Enable
_A_CUSTOMIZ	All Customizing Access - Complete IMG Access	High	 Enable

NOTE: If the status of a Critical Role or Critical Profile is set to Disabled the Role or Profile is not included when running a Critical Roles/Profiles Risk Analysis.

Defining and Maintaining Object Rules

Object Rules matrices can be used in place of the standard (Global) Authorization Object Level Rules generated when creating Risks.

Compliance Calibrator supports the use of five separate Object Rule matrices. Each matrix can be applied instead of the standard (Global) Object Level Rules table when running a Risk Analysis. See Choosing a Rules Matrix for more information about using the Global or alternate Object Rules matrices.

Building an SoD Supplementary Table

The SOD Supplementary table is used to exclude or include Users when running a Risk Analysis.

The SoD Supplementary table can be used when additional security parameters have been defined. When running a Risk Analysis records in the SoD Supplementary table means additional processing is required to identify a SoD. The SoD Supplementary table can also be used to exclude Users that do not have SoDs.

- **Risk ID** - This field specifies the Risks to be processed during Risk Analysis
- **Table Name** - The table you specify in this field must contain the fields specified in Field Name 1, Field Name 2, and User ID Field.
- **Field Name 1, Field Name 2** - These are the fields checked during Risk Analysis
- **Field Value, Field Value** - These fields contain the values for the fields specified in Field Name 1 and Field Name 2.
- **User ID Field** - This field specifies the name of the field in the table specified in Table Name.
- **Exclusion Parameter** - This field determines if the SoD is included in the Risk Analysis report. Leaving the field blank means to include the SoD from the report if all the other field values in the Supplementary record are met. If you set the Exclusion parameter to NOT the SoD is excluded in the Risk Analysis report, if all the other field values in the Supplementary record are met.

During a User-based Risk Analysis, if a SoD is identified, the Supplementary table is searched. If the SoD is in any record of the table (specified in the Risk ID field) the additional processing based on the Supplementary table record is performed:

1. Locate any records in the Supplementary table that specifies the SoD in the Risk ID field and continue processing those records.
2. If the User ID associated with the identified SoD is a value in the field specified in the User ID field, process that record.
3. If the Field Values for Field Name 1 and Field Name 2 match for the User ID, then exclude or include the SoD in the Risk Analysis report based on the value in the Exclusion Parameter field.

NOTE: You MUST enter values in Field Name 1, Field Value (1), Field Name 2, and Field Value (2). Even if the field values are identical all four fields must contain values for the table entry to be valid.

Configuration Options

In order for the values in the SoD Supplemental table to be applied during a Risk Analysis you must set the Configuration Option Use SoD Supplementary Analysis to YES.

Defining and Maintaining Organizational Rules

You can define and maintain your Organizational Rules through the Rule Architect or you can create them with a spreadsheet program and then upload the data into Compliance Calibrator.

Using Organizational Rules

Compliance Calibrator's Organizational Rules provide the capability to isolate Risk Analyses to specific Organizational Levels within your organization. Organizational Rules are used when running a User-based Risk Analysis. See Choosing a Report Type for more information about using Organizational Rules when running a Risk Analysis.

The Rules defined in the Organizational Rules table work in conjunction with the ORGUSERS table.

- The ORGUSERS table contains records storing a user's organizational level field values.
- The Organizational Rules table contains records defining the following criteria-
 - The organizational level field values used to determine which users from the OrgUsers table should be included in the Risk Analysis when the Organizational Rule ID is specified.
 - The Risk IDs the Organizational Rule should be applied to during Risk Analysis

When you apply an Organizational Rule to a User-based Risk Analysis the following process occurs before the Risk Analysis report is generated.

- A run-time Authorization Object Level Rules table is generated for the range of Risk IDs specified in the Organizational Rule. This run-time table is similar to the standard Authorization Object Level Rules. The difference is any Object Level Rule generated from an object containing an organizational level value. The run-time Rules table replaces the variable from the standard object Rules table - in this case \$BUKRS, with the Organizational Level field values specified in the Organizational Rule in this case "US01".
- Step two of the process checks the records in the OrgUsers table. Only those users in the OrgUsers table with an organizational level value matching those specified in the Organizational Rule - in this case the value "US01" in the organizational level BUKRS field will be included in the Risk Analysis.

NOTE: If you include a user in the Risk Analysis and the user does not have a record in the ORGUSERS table the user is not included in the analysis.

- The Risk Analysis then generates the report. The report contains all SoDs for the users included in the analysis with the exception of the Risks specified in the Organizational Rule - in this case those Risks beginning with ID P001 (remember object level Rules have nine characters). Those Risks specified in the Organizational Rule are only included in the Risk Analysis report if they meet the additional test of the organizational level field value - in this case "US01".

The fields in each record of the Organizational Rules table are used in the following way:

- **Org. Rule ID** - This field stores your customized ID number. An ID can be ten characters long. You should establish a naming convention for your

Organizational Rule IDs. That way you can use wildcards to specify multiple Organizational Rules when running a Risk Analysis.

- **Risk ID** - These are the Risks filtered by the Organizational Rule. See above for an explanation of how Organizational Rules are used. You can use the '*' wildcard when specifying a Risk ID.
- **Field** - This field specifies the organizational level variable. When you specify an Organizational Rule when running a Risk Analysis the value in this field is replaced with the actual value contained in the Organizational Level field of each User record in the OrgUsers table.
- **From and To** - These fields specify the values to look for in the User's Organizational Value field contained in the OrgUsers table.
- **AND/OR/NOT** - The default value in this field is AND. If you leave the field blank AND is assumed. If the field is set to AND, the values in the From and To fields are combined and the User is included in the Risk Analysis, then all the values appear in the User's Organizational Value field. If the field is set to OR, the values in the From and To fields are separated and a Risk is generated when running a Risk Analysis, then any of the values in the From and To fields appear in the User's Organizational Value field. If the field is set to NOT, a Risk is generated when running a Risk Analysis, then any values other than the ones specified in the From and To fields appear in the User's Organizational Value field.
- **Rule Description** - This field stores your customized description of the Rule.
- **Status** - This field can be set to Enable or Disable. Only enabled Rules affect a Risk Analysis.

Creating a Transport Request for Rule Architect Tables

You can use the Mass Transport menu item under the Utilities menu to create a transport for all tables maintained through Rule Architect.

If you know the Request ID you want to use for the transport you can enter it, or you can create a new request.

The following files are included in the transport :

- /VIRSA/BUSSPROC - This table stores the list of Business Processes.
- /VIRSA/COUPLETCDD - This table stores all coupled transactions.

NOTE: The Coupled Transaction feature is not available in SAP Compliance Calibrator by Virsa Systems version 4.6.b. The feature is available in version 4.6c and higher.

- /VIRSA/FUNCTBP - This table stores the relationship between Business Processes and Functions.
- /VIRSA/FUNCTION - This table stores the list of Functions.
- /VIRSA/FUNCTOBJ - This table stores the relationship between Function, transaction code and authorization objects.
- /VIRSA/FUNCTRISK - This table stores the relationships between Functions and Risks.
- /VIRSA/FUNCTTCD - This table stores the relationships between Functions and transaction codes.
- /VIRSA/ORGRULES - This table stores all the Organizational Rule records.
- /VIRSA/RISKS - This table stores a list of all Risks.
- /VIRSA/TCODE - This table stores the list of transaction codes and customer descriptions entered in a Function.
- /VIRSA/ZCRAUTH - This table stores all the Authorization Object Rules.
- /VIRSA/ZCRAUTHL1 - This table stores the Matrix 1 Authorization Object Rules.
- /VIRSA/ZCRAUTHL2 - This table stores the Matrix 2 Authorization Object Rules.
- /VIRSA/ZCRAUTHL3 - This table stores the Matrix 3 Authorization Object Rules.
- /VIRSA/ZCRAUTHL4 - This table stores the Matrix 4 Authorization Object Rules.
- /VIRSA/ZCRAUTHL5 - This table stores the Matrix 5 Authorization Object Rules.
- /VIRSA/ZCRPARAM - This table stores all the SoD Supplementary records.
- /VIRSA/ZCRPROF - This table lists all the records in the Critical Profiles table.
- /VIRSA/ZCRROLES - This lists all the records in the Critical Roles table.
- /VIRSA/ZCRTRAN - This lists all the records in the Critical Transactions table.
- /VIRSA/ZSODTC - This table stores all the conflicting transactions.

3. Managing Controls

Introduction

There may be circumstances and times when you want to allow certain combinations of transactions identified as SoDs to be available to specific Users, Roles, or Profiles. You can mitigate the Risks identified with any User, Role, Profile, or HR Object by assigning a Mitigation Control.

A Mitigation Control performs the following function -

- The Control marks an SoD as a known Risk.
- It establishes a period of time the Risk may exist (is monitored).
- The Mitigation Control associates a list of Monitors with the Control. Only Monitors associated with a Control definition may be selected when mitigating a Risk.
- The Mitigation Control specifies a list of Report transactions to be executed to monitor the use of the conflicting transactions associated with the Risk.

Compliance Calibrator Mitigation Controls can be assigned to Users, Roles, Profiles, or HR Objects to mitigate a Risk. When you mitigate a Risk by assigning a Control an email is sent to the Monitor you selected from the list of associated Monitors.

Compliance Calibrator permits only defined Mitigation Controls to be applied to a Risk i.e. a Risk identified through Risk Analysis cannot be mitigated unless the Control has been previously defined.

Mitigation Controls Module Features

The Mitigation Controls module provides the following functionality -

- Establish a list of Monitors- These are the people who will be associated with specific Controls. When the Control is assigned to a User, Role, Profile, or HR Object the associated Monitor is notified by email.
- Establish a list of Approvers - Approvers are associated with specific Controls and are responsible for approving the definition of a Control.
- Create a list of Business Units- Business Units segment your organization so Controls, Approvers, and Monitors can be categorized. It also provides the ability to define which Controls are available for mitigation through Compliance Calibrator Security Role assignment.
- Define your Mitigation Controls - This is where you'll create your Controls, associate each with a particular Business Unit and Approver, determine which Risk IDs can be mitigated by the Control, and associate one or more Monitors with the Control.
- Review Risks/Control relationships - The records in this table store the relationships between Controls and Risk IDs. These relationships are created when you define your Mitigation Controls. For each Risk ID associated to a Control another record is added to this table. You can associate more than one Risk ID to a Control.
- Review Monitors/Control relationships - The records in this table store the relationships between Controls and Monitors. These relationships are created when you define your Mitigation Controls. Each time you associate a Monitor to the Control another record is added to this table. You can associate multiple Monitors with a Control.
- Assign Controls to Users, Roles, Profile, and HR Objects - When you run a Risk Analysis at Authorization Object level you can mitigate any SoD listed in the Risk Analysis report. You also have the ability to assign a Control during the definition of the Mitigation Control by using the buttons at the bottom of the Control definition form.
- Review Invalid Mitigation Controls - This is where you can review the four reports on invalid controls. When you define a Mitigation Control

you specify the lifespan of the Control by establishing validity dates. Any Controls with expired validity dates appear in these reports.

- Maintain Controls Offline and Create Control Transports- You'll use these tools to archive and maintain your Mitigation Control tables offline and prepare transports.

Mitigation Controls Library

When you first enter the Mitigation Controls module the Controls Library is displayed. The Controls Library lists all the existing Mitigation Controls and sorts the Controls by

- Risk
- Risk Level
- Business Unit
- Monitor
- User, Role, Profile, or HR Object

Defining and Maintaining Monitors and Approvers

Monitors are responsible for monitoring the use of transactions associated with a Risk when it is assigned to a Mitigation Control. Approvers are responsible for approving the definition of a Mitigation Control i.e. all the Risks and reporting transactions associated with the Control.

In order to assign Monitors and Approvers to Mitigation Controls you must first establish a list of authorized Monitors and Approvers.

1. To create your list of Monitors click Define Monitors and Approvers on the Mitigation Control menu. The Mitigating Monitors and Approvers table is displayed.
2. Click New Entries to add a record to the table.
3. Click in the Monitor ID field and then click the Search button. This displays all the known User IDs.
4. Enter the first and last name of the Monitor or Approver.
5. Enter the User's email address.
6. Choose a Role for the new Monitor or Approver.
7. Click Save after you've created all the Monitors or Approvers you need. The Monitors and Approvers appearing in this table can be assigned to the Mitigation Controls you'll define.

Figure 3–1: Defining Monitors and Approvers

Mitigating Monitors and Approvers			
Monitor Id	Complete name	Email Id	Role
MITIGATION	Mitigation Monitoring	ccmitigation@virsa.com	Both
PL4500	Jack Foster	jfoster@virsa.com	Both
PL4700	Peter Coleman	pcoleman@virsa.com	Both

Defining and Maintaining Business Units

Establishing Business Units allows you to categorize your Mitigation Controls. When you define your Mitigation Controls you'll categorize them by assigning each one to a specific Business Unit. This enables you to limit the Controls available to the Business Units specified in a Compliance Calibrator Role definition. Refer to the Compliance Calibrator Security Authorizations Guide for more information about Compliance Calibrator Role definitions.

Configuration Options

The configuration option Enable Business Unit Authority Check must be turned on (set to YES) in order to limit access to Mitigation Controls by

Business Unit. If this parameter is set to YES the Mitigation Controls available are limited to those specified in the assigned Compliance Calibrator Role. If it is set to NO the Business Units specified in the Compliance Calibrator Role definition do not limit the Mitigation Controls available for use.

Each Business Unit you define has its own ID.

1. Click Business Units and then click Define in the Mitigation Controls menu.
2. Click New Entries.
3. Enter an ID.
4. Enter a description.
5. Click Save once you've defined all your Business Units.

Assigning Approvers to Business Units

Approvers must approve the definition of a Mitigation Control before it can be assigned to a Risk. You can limit the Mitigation Controls an Approver may approve by categorizing each Approver to a Business Unit.

Defining Mitigation Controls

When you define a Mitigation Control you create a Mitigation Control ID. This Control ID appears in various Risk Analysis reports.

Defining a Mitigation Control includes associating the Risk IDs that may be mitigated by the Control. Only the Risk IDs associated in the Control definition may be mitigated by the Control.

Click Mitigation Controls on the toolbar and then click Create to display the Control Definition form.

NOTE: While initially defining the Mitigation Control, if you click Save your new Control is saved. If you want to make any changes or additions to the Control you need to reopen the Control through the Display/Change form.

Figure 3–2: Creating a Mitigation Control

The screenshot shows the 'Maintain Mitigating Control' SAP form. The header section includes fields for 'Mitigating Control Id' and 'Description'. Below these are 'Business Unit' and 'Management Approver' fields. A tabbed interface is present with 'Associated Risks', 'Monitors', and 'Reports' tabs. The 'Associated Risks' tab is active, showing a table with columns 'Risk Id', 'Risk description', and 'Level'. At the bottom of the form are buttons for 'Save', 'Cancel', 'Mitigate Users', 'Mitigate Roles', 'Mitigate Profiles', and 'HR Mitigation'.

There are four sections in the Mitigation Control definition form -

Header Section - This section contains four fields -

- **Mitigation Control ID** - This is a unique ID created to reference the Mitigation Control. The Mitigation Control ID can be ten characters long. This ID appears in Risk Analysis reports if the Control has been assigned to a User, Role, Profile, or HR Object.
- **Description** - This field is used to describe the uses of the Control. The description is informational only and does not restrict the use of the Control. The description should be something meaningful from a business sense. The description appears in certain reports along with the Mitigating Control ID and makes it easy to understand the use of the Control.
- **Business Unit** - This field has a drop-down menu containing all the defined Business Units. Business Units are used to restrict the use of Mitigation Controls through Compliance Calibrator Security Roles.
- **Management Approver** - This field has a drop-down menu containing all the defined Approvers. See section 2.2, Defining and Maintaining Monitors and Approvers for more information. Before a Control may be used to mitigate a Risk the Control definition must be approved.

Associated Risks Tab - This section is used to associate Risk IDs with the Mitigation Control. Only Risk IDs associated with a Control may be used to mitigate a Risk. This tabbed section contains three fields -

- **Risk ID** - You can click the Search button to display a list of Risk IDs or enter a Risk ID manually. The Risk IDs you specify here are considered associated with the Control and have not been assigned to any User, Role, Profile, or HR Object Risk. Until you mitigate a Risk from a Risk Analysis report or mitigate a Risk by clicking one of the four buttons at the bottom of the Control definition form, Risk IDs listed here are only associated with the Control. You must associate Risk IDs with a Control before you can mitigate the Risk.
- **Risk Description and Level** - These fields are filled in by Compliance Calibrator from the Risk Description you created and the Risk Level you

specified when you defined the Risk. See section 1.9, Defining Risks for more information.

When you Save the Control a record is added to the Risk/Control table. See section 2.8, Reviewing Risk and Control Relationships for more information. A record is also added to the Monitor/Control table for each Monitor you associate with the Control.

NOTE: When you associate Risk IDs with a Control you specify the Risk ID. A Risk ID is a four character ID. When you run a Risk Analysis at SoD Authorization Object Level SoDs are identified with a nine character Risk ID. In order to mitigate the Risk through the Risk Analysis report you must either specify the nine character ID or use wildcards e.g. F001*.

Monitors Tab - This section is used to associate Monitors with the Mitigation Control. This tabbed section contains one field -

- Name - This field has a drop-down menu containing the names of all the Monitors you defined. See section 2.2, Defining and Maintaining Monitors and Approvers for more information. You can associate multiple Monitors with the Control. When you mitigate a Risk you can choose which associated Monitor you want to be responsible for mitigating the specific Risk.

Reports Tab - This section is used to specify the Report transactions to be run in order to monitor the use of the conflicting transactions defined by the Risk IDs. This tabbed section contains four fields -

- Transaction Code - Click in the field and click the Search button to find the transaction you want to add, or just enter the transaction code.
- Description - This field is filled in by Compliance Calibrator. It is the SAP description associated with the Report transaction.
- Monitor - This field has a drop-down menu containing all the Monitors you defined. See section 2.2, Defining and Maintaining Monitors and Approvers for more information. This is the person responsible for running the Report transactions.
- Frequency - This field specifies how often, in days, the Report transaction should be run.

NOTE: The Frequency value also determines whether an Alert is generated. If a Report transaction is not run within the time specified by the Frequency value an Alert is sent to the manager specified in the Alerts module. See section 3.1, Assigning Alert Monitors for more information.

Mitigating Users, Roles, Profiles, and HR Objects

Once you have defined a Mitigation Control you can assign it directly to a User, Role, Profile, or HR Object. You can assign the Control without running a Risk Analysis by clicking the appropriate button at the bottom of the Mitigation Control form.

NOTE: If the following configuration options are set to YES your ability to assign a Control to a User, Role, or HR Object is limited by the Compliance Calibrator Role assigned to your User ID. Refer to the Compliance Calibrator Security Authorizations Guide for more information on Compliance Calibrator Roles.

- Enable User Group Authority Check for Mitigation
- Enable Risk Level Authority Check for Mitigation
- Enable Role Level Authority Check for Mitigation
- Enable HR Object Level Authority Check for Mitigation

Maintaining Mitigation Controls

Once a Mitigation Control has been created you can view or change its definition, or delete the Control. Click Mitigation Controls on the toolbar and then click Display/Change to search for and display a Control.

You can redefine any part of a Mitigation Control except its ID.

NOTE: If a Mitigation Control is assigned to a User, Role, Profile, or HR Object you cannot delete the Control.

Reviewing Risk and Control Relationships

The Risk/Control table displays all the Risk IDs associated with Controls. The records in this table are created when you associate a Risk ID through the Mitigation Control definition form.

NOTE: This table is not maintained directly. If you want to change or remove a record from this table make a change to the Mitigation Control definition by adding or removing a Risk ID. See section 2.7, Maintaining Mitigation Controls for more information about maintaining Mitigation Controls.

Reviewing Monitor and Control Relationships

The Control/Monitor table displays all the Control and Monitor relationships created when you defined your Mitigation Controls. The table is used to review the related Controls and Monitors.

NOTE: This table is not maintained directly. If you want to change or remove a record from this table make a change to the Mitigation Control definition by adding or removing a Monitor. See section 2.7, Maintaining Mitigation Controls for more information about maintaining Mitigation Controls.

Reviewing Controls Assigned to Users, Roles, Profiles, and HR Objects

You can review and maintain all the assigned Mitigation Controls through the User, Role, Profile, and HR Object Mitigation tables. These tables allow you to change the validity dates of a Control, the monitor assigned to the specific instance of the Control, and if the instance is enabled or disabled.

Control Reports

The Expired Mitigation Controls report lists Mitigation Controls whose validity dates have expired. The report is broken down by Users, Roles, Profile, and HR Objects. All four are line item reports.

Each report displays the following information:

- Mitigation Controls - Each report lists the Mitigation Control ID and its description.
- Risk - Each report includes the Risk ID, description, and Risk Level
- Validity Dates - Each report includes the period of validity.
- Monitor - Each report includes the User ID of the Monitor for the Control.
- Status - The status is also included in the report. An 'Enable' status means the Control is available for mitigation. A Mitigation Control with an 'Enable' status appearing in the Invalid Mitigating Control report may have its validity dates changed. A Mitigation Control with a 'Disable' status means the Control can not be used for mitigation.

Figure 3–3: Expired Mitigating Controls for Roles

Z_AP_ACCOUNTANT		Description : Accounts Payable Accountant	
Mitigating Control	Risk Description	Level	Validity
000001: and is compared to the previous days processed documents. It is then signed by the reviewer and for review by Plant Compliance and Internal Audit.	P001*: Create fictitious vendor and initiate payment to the vendor	High	01/01/2005 - 03/09/2005

Figure 3–4: Expired Mitigating Controls for Profiles

MMAN7MODEL		Description : Profile for role VMAN07PHIV_VRMINGMT		
Control	Risk Description	Level	Validity	Monitor
	M00604201: Receive/issue incorrect amount and adjust via VM stock count I	High	02/16/2005 - 03/09/2005	EMPL4500

Maintaining Control Tables Off-Line

Downloading and uploading Control data tables makes it easy to archive your Control data and also share the data from one Compliance Calibrator system installation and another. Data can be built on a development system and then moved to different production systems.

The tables used to store Control data can be downloaded and maintained through a spreadsheet program. Once you have made any changes or additions to the tables you can upload the tables and Compliance Calibrator can use the updated data.

Use the Upload and Download menu items to perform the required task for each table you want to maintain.

Creating a Transport Request for Mitigation Control Tables

You can easily move data from one system to another using the Mass Transport. Mass Transport includes all the Control tables in the transport request you create.

If you know the Request Number you want to use enter in the Request field. You can also create a new Transport Request by clicking the Own Requests button.

The following files are included in the transport:

- /VIRSA/BUAPPVR - This table stores the relationships between Business Units and Approvers.
- /VIRSA/BUMONITOR - This table stores the relationships between Business Units and Monitors.
- /VIRSA/MITREPORT - This table stores the information from the Mitigation Control Reports tab.
- /VIRSA/ZBUSUNIT - This table stores the list of Business Units.
- /VIRSA/ZMITAPVR - This table stores the information from the Mitigation Control Monitors tab.
- /VIRSA/ZMITMON - This table stores the list of Monitors.
- /VIRSA/ZMITREF - This table stores the Mitigation Control header information i.e. Control ID, Description, Business Unit, and Management Approver.
- /VIRSA/ZMITRISKS - This table stores the information from the Mitigation Control "Associated Risks" tab.

4. Managing Alerts

Introduction

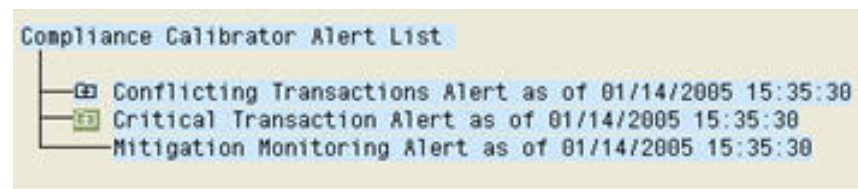
An Alert can be generated for three different reasons -

1. Executing a Conflicting transaction - These transactions are maintained through Rule Architect.
2. Executing a Critical transaction - The Critical transactions table is maintained through Rule Architect.
3. Not running specified Report transactions within a given time period - These transactions are maintained through the Mitigation Controls module.

NOTE: Report transactions are determined through Mitigation Control definitions. The time period is specified in the Frequency field of a report transaction. See section 2.5, Defining Mitigation Controls for more information.

Alerts are listed in the Compliance Calibrator Alert module and can also be sent as emails.

Figure 4-1: Compliance Calibrator Alert Tree



Assigning Alert Monitors

The Alert Monitor table is used to assign monitors to either a Critical or Conflicting transactions, or the Mitigation Control containing the Report transactions to be monitored.

Figure 4-2: Assigning Alert Monitors

Risk Id	Mit Control Id	Email Id	User
0001*		jfooster@virsasystems.com	Jack Foster
	MCFI0001	jfooster@virsasystems.com	Jack Foster

Each record in the table either specifies an Alert monitor for Critical or Conflicting transactions or a Mitigation Control Report transaction.

A record cannot specify an Alert monitor for Critical/Conflicting transactions and Mitigation Control Report transactions. If you want to assign the same person as a Critical/Conflicting transactions Monitor and as a Mitigation Control Report Transaction Monitor, create two records in the table.

Each record in the table has three fields -

- If you are assigning a monitor to a Critical or Conflicting transaction, enter the Risk ID of the transaction. Leave the Mitigation Control ID field

blank. This Risk ID was created through the Rule Architect. You can use wildcards. The Risk ID must be at least two characters long; e.g. F*.

- If you are assigning a monitor to a Mitigation Control Report Transaction, enter the Mitigation Control ID. Leave the Risk ID blank. The Mitigation Control ID must be at least two characters long; e.g. M*
- Enter the email address of the person who should receive the alert.

NOTE: You can assign more than one monitor to a Risk ID or Mitigation Control ID by creating multiple records in this table.

Monitoring Conflicting Transaction Alerts

When a Conflicting transaction is executed the monitor(s) assigned to the transaction are notified by email.

Figure 4–3: Email Alert for Conflicting Transactions

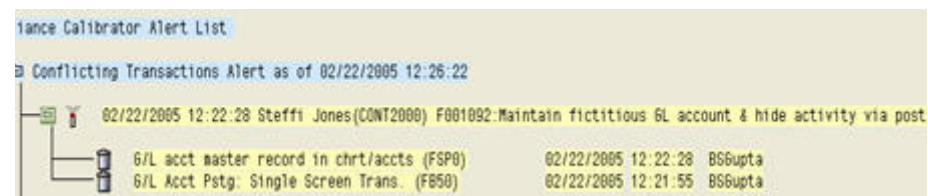
```

Conflicting Transactions Alerts **

ER : Bhanu Mohanty (BMOHANTY)
sk : FO10 - MAINTAIN PROJECT and MAINTAIN WBS
ansaction : Create Work Breakdown Structure (CJ01) Date : 12/28/2004 Time : 10:32:48
ansaction : Create WBS Element (CJ11) Date : 12/28/2004 Time : 10:32:55
  
```

Monitors can also review the list of alerts through Compliance Calibrator's Alerts module. Click Alerts on the control panel toolbar and click the plus sign next to Conflicting Transactions.

Figure 4–4: Monitoring Conflicting Transaction Alerts



Each Conflicting transaction Alert has two parts -

Alert Header - This contains the following Alert information -

- Time and date the Alert was generated
- The User name and User ID of the person who caused the Alert to be generated
- The transaction level Risk ID and the Risk ID description

To the left of each Alert Header is the lighted matchstick icon. You can click the icon to clear the Alert. You can view cleared Alerts by clicking Cleared Alerts on the toolbar.

Clearing an Alert has the following effect -

- If the both transactions that make up the conflicting transaction pair are executed again a new Alert is generated.

Alert Body - This contains information about each transaction executed in the set of conflicting transactions

- Transaction code and Transaction description for each transaction executed in the set of conflicting transactions.
- Time and date for each transaction executed in the set of conflicting transactions
- Name of the Monitor responsible for the Alert e.g. BSGupta

To the left of each conflicting transaction in the Alert Body is a garbage can icon. If you click the icon the corresponding transaction is deleted.

Deleting individual conflicting transactions has the following effect -

- If the deleted transaction is executed again by the same User a new Alert is generated. By deleting the individual transaction from the conflicting transaction pair you are specifying the undeleted transaction is still active and an Alert is necessary for this User the next time the individual transaction is executed.

Deleting both conflicting transactions from the Alert has the following effect -

- If either of the deleted transactions are executed again by the same User a new Alert is not generated. Both transaction that make up the set of conflicting transactions must be executed to generate an Alert.

Monitoring Critical Transaction Alerts

When a critical transaction is used the monitor(s) assigned to that transaction are notified by email.

Figure 4–5: Email Alert for Critical Transactions

```

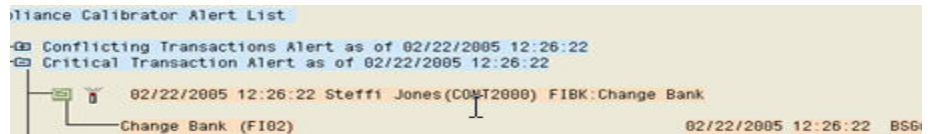
Critical Transaction Alerts **

ER : Brenda King (BKING)
sk : T001 - User Maintenance - Should be restricted to User Admins on
ansaction : User Maintenance (SU01)  Date : 12/28/2004  Time : 11:01:

ER : Bhanu Mohanty (BMOHANTY)
sk : T001 - ABAP Editor - System stabilitiy & integrity at risk
ansaction : ABAP Editor (SE38)  Date : 12/28/2004  Time : 11:12:27
  
```

Monitors can also review the list of alerts through Compliance Calibrator's Alerts module. Click Alerts on the control panel toolbar and click the plus sign next to Critical Transactions.

Figure 4–6: Monitoring Critical Transaction Alerts



The screenshot shows the 'Compliance Calibrator Alert List' window. It displays two alerts: 'Conflicting Transactions Alert as of 02/22/2005 12:26:22' and 'Critical Transaction Alert as of 02/22/2005 12:26:22'. The second alert is expanded, showing a table with one entry: '02/22/2005 12:26:22 Steffi Jones (C04T2000) FI8K:Change Bank'. Below this, a link 'Change Bank (FI82)' is visible. The date and time '02/22/2005 12:26:22' and the monitor name 'BSG' are also shown.

Each Critical transaction Alert has two parts -

Alert Header - This contains the following information:

- "Time and date the Critical transaction was executed
- "Name and User ID of the person executing the Critical transaction
- "The transaction code and the transaction description

Alert Body - This contains the following information:

- The transaction description and the transaction code of the Critical transaction
- Time and date the Critical transaction was executed
- The User ID of the monitor responsible for the Alert

Each critical transaction alert lists the transaction used and can be cleared by clicking the matchstick icon.

NOTE: Whether or not a Critical transaction Alert has been cleared does not affect the generation of another Alert for the same Critical transaction being executed by the same User.

Monitoring Activity Control Alerts

Report transactions are included when defining a Mitigation Control. Each Report transaction has a Frequency value which determines how often the Report transaction should be run. If a Report transaction has not been run within the required number of days an Alert is generated and emailed. Each Monitor Control Alert has two parts -

Alert Header - This contains the following information:

- The date and time the Alert was generated
- The name of the person who caused the Alert
- The Mitigation Control ID and description

Alert Body - This contains the following information:

- The Report transaction code and description
- The time and date of the last execution of the Report transaction
- The name of the computer the Report transaction was executed from
- The Report Transaction Frequency value - this is the value specified in the Mitigation Control definition

NOTE: In order for the Alert to be generated the Monitor assigned to the Report transaction in the Mitigation Control definition must run the Report transaction once after being assigned. This initial Report transaction execution sets a baseline for the Frequency value.

Reviewing Cleared Alerts

Cleared alerts can be viewed by clicking Cleared Alerts on the toolbar and then using the search form.

5. Running Risk Analyses

Introduction

Risk Analyses are run to see if any User, User Group, Role, Profile, or HR Object has access to two or more transactions defined as conflicting. When two or more transactions are determined to be conflicting the combination of those transactions are defined as Risks. Rules, also called SoDs (Segregation of Duties) are defined by Risks.

When you run a Risk Analysis any existing SoDs are reported for each User, Role, Profile, or HR Object included in the analysis.

Risk Analysis can be run from the SAP R/3 module of Compliance Calibrator or from the HR module. In addition to Roles and Profiles the SAP R/3 module allows you to run Risk Analyses for Users and User Groups and the HR module allows you to run Risk Analyses for HR Objects. When you run a Risk Analysis for HR Objects you must also specify the Object type -

Risk Analysis Types for the SAP R/3 Module
Risk Analysis Types for the HR Module

Figure 5–1: Risk Analysis Types for SAP R/3 and HR Modules

Risk Analysis Types for the SAP R/3 Module	Risk Analysis Types for the HR Module
• Users	HR Object Types
• User Groups	• Job
• Roles	• Organizational Unit
• Profiles	• Position
	• HR Object
	• Roles
	• Profiles

Table 5-1: Object Types and Groups

Users HR Object Types	User Groups Job
Roles Organizational Unit	Profiles Position
HR Object	Roles
Profiles	

In order to perform a Risk Analysis you must specify all the values for the components used to generate the analysis. All the components are defined below.

Choosing an Analysis Type

Compliance Calibrator reports may be run for individual or range of Users, User Groups, Roles, Profiles, or HR Objects.

NOTE: When you run a Risk Analysis from the HR module the Object IDs you choose must match the Object Type.

Configuration Options

The following Configuration Options affect the values you choose for Analysis Type -

- Threshold Value for User Analysis
- Threshold Value for Roles/Profiles Analysis
- Memory Variable for Batch Size
- Show All in Report
- Include Reference User in User Analysis
- Use AND Option in Users & User Groups

NOTE: If you specify a range with a large number of Users, Roles, Profiles, or HR Objects you might want to run the analysis in background mode. See section 4.10, Running Risk Analyses in Background Mode for more information.

Combined Analysis

The Combined Analysis checkbox only affects your Risk Analysis when you include a range of Users, User Groups, Roles, or Profiles.

If you choose to run the analysis for a range and check Combined Analysis all the Users, Roles, or Profile are treated as a composite rather than individually. This means all the transactions and Authorization Objects available to all Users, Roles, or Profiles within the specified range are treated as a composite group.

The report generated from running a Risk Analysis will contain a different set of SoDs than if you ran the Risk Analysis against a range of individual Users, Roles, or Profiles.

You can enter the User IDs, Roles, or Profiles, or choose them from the Search list.

HR Object Based Only

This checkbox only affects Object ID-based analysis.

Leaving this box unchecked and running a Risk Analysis produces a SoD line item report listing all the User IDs associated with the HR Objects you included in the report.

Checking this box and running a Risk Analysis produces a line item report listing the SoDs for the HR Objects you included in the report.

Choosing an SoD Risk Level

Risk Levels are assigned to Risks when the Risk is defined through the Rule Architect. When you run a Risk Analysis you may only want to see SoDs for a certain Risk Level. Choosing a specific Risk Level, rather than choosing "All" filters the SoDs appearing in the Risk Analysis report.

Configuration Options

The following Configuration Options affect the values you choose for Report Type:

- **Default Type of Report**
The report type you choose determines what kind of report is generated when you click the **Execute** button.
- **SoD at Transaction Code Level** - Generating this report type for a User, Role, Profile, or HR Object produces a list of SoDs at transaction level.
- **SoD at Authorization Object Level** - Generating this report type produces a list of SoDs at object level.
- **Critical Transactions** - Generating this report type limits the list to Critical transactions available to the User, Role, Profile, or HR Object. Critical transactions are defined and maintained through the Rule Architect's Critical Transactions table.
- **Critical Roles/Profiles** - Generating this report type lists only the Critical Roles and Profiles associated with the User, Role, Profile, or HR Object. This report does not list any Risks. Critical Roles and Profiles are defined and maintained through the Rule Architect's Critical Roles table and Critical Profiles table.
- **Mitigating Controls** - Generating this report type lists valid Mitigation Controls assigned to the User, Role, Profile, or HR Object included in the analysis.

Filtering Reports by Risk

You can determine which Risks are included in a report by applying a Risk ID filter. By entering a Risk ID or range of Risks IDs only those Risks are considered when you run the Risk Analysis.

The Risk ID field accepts wildcards so you can limit the Risk Analysis to a range of Risk IDs e.g. F001*.

The Risk filter only applies to the following report types. The other report types do not generate Risk information.

- SoD at Transaction Code Level
- SoD at Authorization Object Level
- Critical Transactions

Filtering Reports by Organizational Rule

You can limit the Users included in a Risk Analysis by specifying an Organizational Rule ID. Organizational Rules determine which Users are included in the Risk Analysis by Organizational Level values. See section 1.17, Defining and Maintaining Organizational Rules for more information.

Choosing a Report Format

There are three basic report formats -

- **Business** - The Business report format contains descriptive information about the Risks being reported. This report format has two views - Summary and Detail. The Detail view lists each Risk as a separate line item. The Summary view lists the combination of conflicting transactions that produce the Risk in one line item.
- **Executive Summary** - This report format lists each risk as a single line item and displays the total number of conflicting transactions producing the Risk.
- **Technical** - This report format contains more detailed, technical information than the Business format. This report format has two views - Summary and Detail. The Detail view lists each SoD as a separate line item. The Summary view groups the transactions producing the SoD into a single line item.

NOTE: Once you generate a Risk Analysis using a particular report format you can always switch between the five formats by clicking the corresponding format button on the Compliance Calibrator

toolbar. See section 6, Risk Analysis Reports for a description of each report.

Configuration Options

The following Configuration Options specify the Report Format defaults -

- Default Report Format
- Set Default Business View

Choosing a User Type

Checking a User Type limits the Risk Analysis to those User Types. The initial setting is Default User Type.

Specifying Exclusions

Locked Users, Users or Roles with expired validity dates and those with valid Mitigating controls may be ignored by selecting the corresponding check boxes.

When you perform a Risk Analysis you can exclude any Users, Roles, or Profiles with Mitigation Controls. If you include the mitigated Users, Roles, and Profiles in your Risk Analysis the SoDs are identified by the Mitigation Control IDs.

Configuration Options

The following Configuration Options affect the initial Risk Exclusion values:

- Set Locked Users
- Set Expired Users
- Set Mitigating Controls

Choosing a Rules Matrix

There are five Rule matrices in addition to the standard (Global) Authorization Object Rules table. Each Rule matrix can contain a different set of Rules. Specify which matrix you want to use in place of the standard Rules table by clicking in the field and then clicking the pop-up menu.

Choosing a System for Analysis

You can choose to run your Risk Analyses for User, Roles, or Profiles that exist on remote systems. When you run a Cross-System Risk Analysis you are using the Compliance Calibrator Rules tables residing on your Local system.

Configuration Options

The following Configuration Options affect Cross-System Analysis:

- Cross-System SoD Analysis
- Cross-System ID

Saving and Using Variants

You can save and reuse variants by entering all the values you want saved in each Risk Analysis component clicking the *Save* button. To reuse the saved values click the Variants button on the toolbar.

Running Risk Analyses in Background Mode

Background reporting allows SoD conflicts to be analyzed for a large number of Users, Roles, Profiles, or HR Objects. All the Risk Analysis components described above are used in the same way to produce foreground or

background reports. The difference is the report format (see section 6.7, Background Reports for more information).

When you run your Risk Analysis in the background you need to name the job used to generate the report. When the report is finished being generated you can use transaction SM37 to view the report.

Using the Enable Delta Analysis Configuration Option

If you have the Configuration Option Enable Delta Analysis set to YES and you are running your first background Risk Analysis you should check Force Full Scan and use the SoD at Authorization Object Level report type (specified in the Report type component of the Risk Analysis control panel).

To insure you are including all Risk information in the Delta Analysis tables set the Risk Level to ALL.

The following options appearing in the Schedule Background Job screen (shown above) are specific to Compliance Calibrator -

- Force Full Scan - If you have the Configuration Option Enable Delta Analysis turned on (see below), checking this option directs Compliance Calibrator to ignore the User, Role, or Profile data stored in the Delta Analysis tables and perform a new analysis on all specified Users, Roles, or Profiles.

CAUTION: If you generate any new Rules after running a Risk Analysis you *must* force a full scan in order to re-analyze all Users, Roles, and Profiles stored in the Delta Analysis tables. To do this, check Force Full Scan when you run the background analysis.

- Process only Changed Users/Roles/Profiles - This option directs Compliance Calibrator to include only those Users, Roles, or Profiles that have changed since the last analysis.
 - The check for changed Users/Roles/Profiles is based on the data stored in the Delta Analysis tables.
 - If you have specified a range of Users/Roles/Profiles and only a subset of them have changed, only the changed Users are included in the Risk Analysis report.
 - If you specify a range of Users/Roles/Profiles and a subset of the range are not in the Delta Analysis tables (Users/Roles/Profiles that have never been analyzed), they are included in the analysis report, even if this option is checked.

NOTE: If you check both options, Process only changed Users/Roles/Profiles is ignored and Force Full Scan is applied.

- Update Management Report - This option updates the statistics in the Compliance Calibrator Statistical report (located on the control panel toolbar).
 - If you are running the background Risk Analysis to update this report do not exclude Locked or Expired Users (check the Exclusions component in the Risk Analysis control panel).
 - If you are running the background Risk Analysis to update this report do not check Process only changed Users/Roles/Profiles.

Configuration Options

The following Configuration Options affect running a background Risk Analysis -

- Enable Delta Analysis
- Batch Size for Users
- Batch Size for Roles
- Multiple Spool Option

WARNING! Running a background Risk Analysis that includes a large number of Users with many SoDs, may cause a memory error. Set the Multiple Spool option to YES to prevent memory errors in these cases.

6. Running Simulations

Introduction

You can run 'what-if' scenarios by simulating the addition of transactions, Roles, or Profiles to existing Users, Roles, or Profiles.

The values for transactions, Roles, or Profiles you enter in the Simulation forms are added to the User, Role, Profile, or HR Object you have entered in the Analysis Type component of the Risk Analysis form.

To run a Simulation Analysis enter the Users, Roles, Profile, or HR Object in the Analysis Type component and click Simulation on the Compliance Calibrator toolbar.

CAUTION: If you are running a User-based analysis and don't enter any User ID the simulation defaults to running the simulation against All Users.

Configuration Options

The following Configuration Options affect Simulations :

- Cross-System SoD Analysis
- RFC Destination for Remote Simulation

Simulating Risks for Users and User Groups

You can simulate adding a Transaction, Role, or Profile to the Users included in your analysis. By entering an individual or range of Transactions, Roles, or Profiles and executing the simulation you can test to see if the additional resources produce any SoDs.

The checkboxes perform the following functions -

- **Exclude Values** - Risk Analysis simulates the removal of the Transaction, Role, or Profile from the User or User Groups you included in your analysis. Excluded SODs are highlighted in the generated report.
- **Risks from Simulation Only** - Risk Analysis reports only the SoDs produced by adding the Transactions, Roles, or Profiles to the Users or User Groups you included in the analysis

NOTE: If both Exclude Values and Risks from Simulation Only are checked, the Exclude Values option is ignored.

Simulating Risks for Roles and Profiles

You can simulate adding a Transaction or Role to the Roles or Profiles included in your analysis. By entering an individual or range of Transactions or Roles and executing the simulation you can test to see if the additional resources produce any SoDs.

NOTE: If you include a composite Role in the Analysis Type component you can't include a composite Role in the Simulation form.

If you include a composite Role in the Analysis Type component and you specify single Roles in the Simulation form, the single Roles are added to the Composite Role for simulation analysis.

The checkboxes perform the following functions -

- **Exclude Values** - Risk Analysis simulates the removal of the Transaction or Role from the Roles or Profiles you included in your analysis
- **Risks from Simulation Only** - Risk Analysis reports only the SoDs produced by adding the Transactions or Roles to the Roles or Profiles you included in the analysis
- **Include Composite Roles** - This checkbox only applies if you are simulating the addition of composite Roles. If it is checked a second report appears below the standard simulation report listing the simulated SoDs for each composite Role.
- **Include Users** - If you check this box you can only run the simulation in background mode. If it is checked an additional report is displayed below the standard simulation report listing the Users for each simulated SoD.

Editing Objects for Simulation

If you are simulating adding or excluding a transaction to a User, Role, Profile, or HR Object and you are going to generate a SoD Authorization Object Level Risk Analysis an additional button, Edit Objects is included on the Simulation form. By clicking Edit Objects the objects associated with the specified transactions can have their field values edited for the simulation.

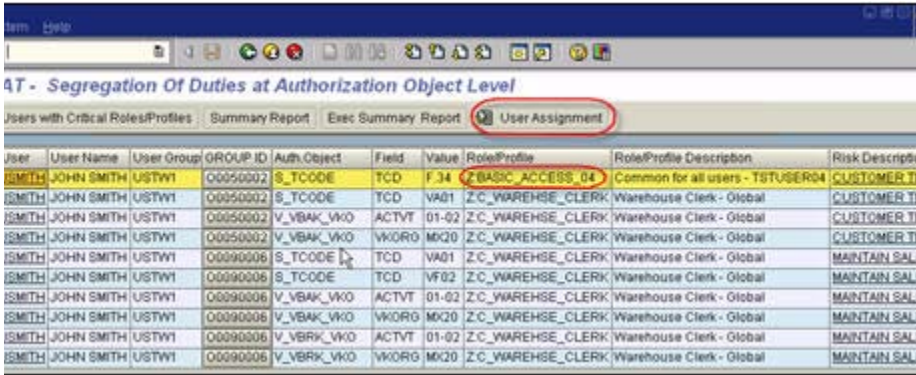
NOTE: You can perform remote simulations by choosing a RFC from the pop-up menu. The remote systems appearing in the pop-up menu must be pre-defined. See Appendix E, Defining RFC Destinations for more information.

Role Assignment through Simulation

When you run a User-based simulation you can perform Role assignment for any simulated Role that does not generate a SoD.

NOTE: Your ability to perform Role assignment through simulation is determined by the Compliance Calibrator Security Role authorizations assigned to your User ID.

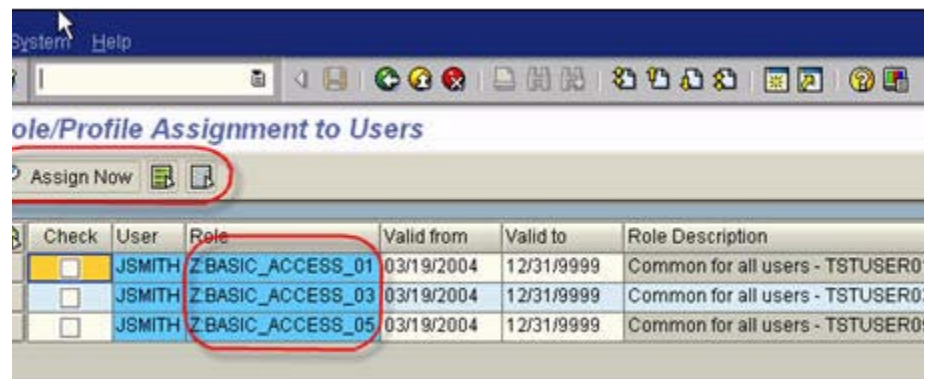
Figure 6–1: Simulation Risk Analysis Report



User	User Name	User Group	GROUP ID	Auth.Object	Field	Value	Role/Profile	Role/Profile Description	Risk Description
SMITH	JOHN SMITH	USTW1	00050002	S_TCODE	TCD	F 34	ZBASIC_ACCESS_04	Common for all users - TSTUSER04	CUSTOMER T
SMITH	JOHN SMITH	USTW1	00050002	S_TCODE	TCD	VA01	ZC_WAREHSE_CLERK	Warehouse Clerk - Global	CUSTOMER T
SMITH	JOHN SMITH	USTW1	00050002	V_VBAK_VKO	ACTVT	01-02	ZC_WAREHSE_CLERK	Warehouse Clerk - Global	CUSTOMER T
SMITH	JOHN SMITH	USTW1	00050002	V_VBAK_VKO	WKORG	MX20	ZC_WAREHSE_CLERK	Warehouse Clerk - Global	CUSTOMER T
SMITH	JOHN SMITH	USTW1	00090006	S_TCODE	TCD	VA01	ZC_WAREHSE_CLERK	Warehouse Clerk - Global	MAINTAIN SAL
SMITH	JOHN SMITH	USTW1	00090006	S_TCODE	TCD	VF02	ZC_WAREHSE_CLERK	Warehouse Clerk - Global	MAINTAIN SAL
SMITH	JOHN SMITH	USTW1	00090006	V_VBAK_VKO	ACTVT	01-02	ZC_WAREHSE_CLERK	Warehouse Clerk - Global	MAINTAIN SAL
SMITH	JOHN SMITH	USTW1	00090006	V_VBAK_VKO	WKORG	MX20	ZC_WAREHSE_CLERK	Warehouse Clerk - Global	MAINTAIN SAL
SMITH	JOHN SMITH	USTW1	00090006	V_VBRK_VKO	ACTVT	01-02	ZC_WAREHSE_CLERK	Warehouse Clerk - Global	MAINTAIN SAL
SMITH	JOHN SMITH	USTW1	00090006	V_VBRK_VKO	WKORG	MX20	ZC_WAREHSE_CLERK	Warehouse Clerk - Global	MAINTAIN SAL

Once the Simulation report is generated you can click the User Assignment button to display the non-violating Roles for each User included in the Simulation report.

Figure 6–2: Assigning Non-Violation Roles to Users



Click each checkbox next to a User you want to assign to a Role and then click the Assign Now button.

NOTE: Please refer to SAP Note #861556 for information regarding the installation procedures for SAP Compliance Calibrator by Virsa Systems.

7. Risk Analysis Reports

Introduction

Compliance Calibrator provides SoD reports in the feature rich ALV format. This includes the ability to filter, sort, and/or download you analysis results to other applications for presentation or further analysis. The reports have drill down capabilities allowing detailed analysis through SUIM and PFCG to determine the root cause of the problem.

There are five report types. See section 4.3, Choosing a Report Type. Each of these reports can be formatted in several ways. See section 4.4, Choosing a Report Format.

- SoD at Transaction Code Level reports
- SoD at Authorization Object Level reports
- Critical Transactions Risk Analysis reports
- Critical Role/Profile reports
- Mitigation Control reports

You can generate reports for Users, User Groups, Roles, Profiles, or HR Objects. The following sections provide a screen shot of each report in each available format.

Reporting Features

- Users highlighted in Blue are Expired Users. Those highlighted in Green are Locked Users. Reference Users appear in Yellow.
- The User ID in User-based reports is a link to additional User information.
- The Role name in Role-based reports is a link to additional Role information.
- The Profile name in Profile-based reports is a link to additional Profile information.
- Business View reports can be printed by right-clicking on the report screen and choosing Print from the pop-up menu.
- Reports run with Combined Analysis checked display "Combined" in place of the User, Role, or Profile name in Technical Summary reports. You can click on the word to drill down and see the list of Users, Roles, or Profiles that were combined.
- In Role-based analysis single roles contained within a composite Role are shown only if all the Roles entered for analysis are Composite roles.
- All Mitigation Control IDs appearing in any report are hyperlinks. When you click on the ID the Control description and validity dates are displayed
- In User-based reports, if an SoD is associated with a Composite role the Composite role name is displayed. If the Composite role has been mitigated, the Mitigation ID is also displayed.

SoD at Transaction Code Level Reports

Table 7-1: Available Report Types

SoD at Transaction Code Level - User - Technical Summary format
SoD at Transaction Code Level - User - Technical Detail format
SoD at Transaction Code Level - User - Business Summary format
SoD at Transaction Code Level - User - Business Detail format
SoD at Transaction Code Level - User -Exec Summary format
SoD at Transaction Code Level - Role - Technical Summary

SoD at Transaction Code Level - Role - Technical Detail
SoD at Transaction Code Level - Role - Business Summary
SoD at Transaction Code Level - Role - Business Detail
SoD at Transaction Code Level - Profile - Technical Summary
SoD at Transaction Code Level - Profile - Technical Detail
SoD at Transaction Code Level - Profile - Business Summary
SoD at Transaction Code Level - Profile - Business Detail
SoD at Transaction Code Level - HR Object - Technical Summary
SoD at Transaction Code Level - HR Object - Technical Detail
SoD at Transaction Code Level - HR Object - Business Summary
SoD at Transaction Code Level - HR Object - Business Detail
SoD at Transaction Code Level - HR Object - Executive Summary

Figure 7–1: SoD at Transaction Code Level - User - Business Summary format

r Id : Mark Smith (COHT1000)		User Group : MM-GL01
Conflicting Transactions	Risk Description	Level
Inventory Recount (LI12) and Inventory Differences VM (LI20) and Goods Receipt for PO (MB01)	M006005: Receive/Issue incorrect amount and adjust stock count	High
Inventory Recount (LI12) and Inventory Differences in MM-IM (LI21) and Goods Receipt for PO (MB01)	M006006: Receive/Issue incorrect amount and adjust stock count	High
Inventory Recount (LI14) and Inventory Differences VM (LI20) and Goods Receipt for PO (MB01)	M006009: Receive/Issue incorrect amount and adjust stock count	High
Inventory Recount (LI14) and Inventory Differences in MM-IM (LI21) and Goods Receipt for PO (MB01)	M006010: Receive/Issue incorrect amount and adjust stock count	High

Figure 7–2: SoD at Transaction Code Level - User -Exec Summary format

Description	Level	No. of Conflicts	No. of Mitigated Conflicts
6:Receive/Issue incorrect amount and adjust stock count	High	28	0

SoD at Authorization Object Level Reports

Mitigation Controls can be assigned to Users, Roles, Profiles, and HR Objects when you generate a SoD at Authorization Object Level report.

Assigning Controls to Risks

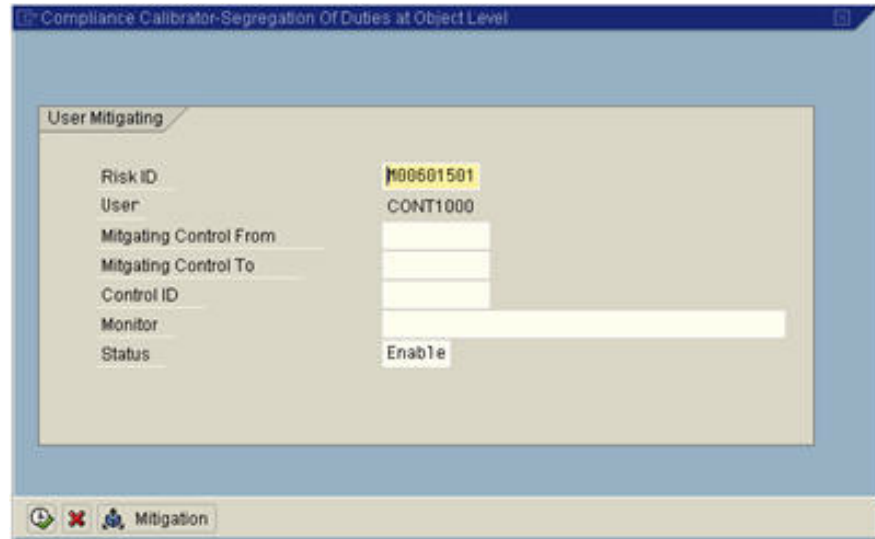
You can assign Mitigation Controls to Risks when you create the Control. See section 2.5, Defining Mitigation Controls for more information. More often you assign your Controls to SoDs when you generate a Risk Analysis report.

You can only assign Controls to SoDs when you have generated the SoD at Authorization Object Level report type.

You can mitigate Risks at transaction-level by editing the Risk ID field shown below. The Risk ID displayed is the nine-character ID associated with the object-level Risk. Transaction-level Risks are seven characters long. By editing the Risk ID you can mitigate at transaction-level; e.g. change M00601501 to M006015, or change it to M00601* to mitigate all transaction-level Risks identified with the User being analyzed.

All of the SoD at Authorization Object Level report examples below display a button in the Risk ID column. When you click the button the Mitigation Control form is displayed -

Figure 7-3: Risk Mitigation from the SoD at Authorization Object Level Report



The screenshot shows a SAP window titled "Compliance Calibrator-Segregation Of Duties at Object Level". Inside is a form titled "User Mitigating". The form has the following fields and values:

Risk ID	M00601501
User	CONT1000
Mitgating Control From	
Mitgating Control To	
Control ID	
Monitor	
Status	Enable

At the bottom of the form is a button labeled "Mitigation".

Enter Validity period "From" and "To" dates.

NOTE: If you have the Date Range Limit for Mitigating Controls option set you don't need to enter any dates. The dates are calculated from the option's value.

Click in the Control ID field and click the pop-up button to display the list of Mitigation Controls associated with this Risk ID.

NOTE: You must have associated the Risk ID with the Mitigation Control when you defined the Control. If this Risk ID is not associated with a Control a message is displayed saying no values were found. If this is the case you can click the Mitigation button and create a new Control, or add the Risk ID to an existing Control. Once you have finished adding or editing a Mitigation Control definition you can use the Back button to return to the Mitigation Control assignment form.

Click in the Monitor field and click the pop-up button to display the list of Monitors associated with the Control you entered. Then click the Execute button to assign the Control to the User, Role, Profile, or HR Object.

Once you assign the Mitigation Control an email is generated and sent to the assigned Monitor. The email contains the following type of information -

Figure 7-4: Email Alert Sent to Mitigation Control Monitor

```

: mitigating control table was updated by JAVILAN on 02/16/2005 at 15:17:1
is email serves as notification that you have been designated as the Monit
: the following User/SOD Conflict

: Mitigating Controls - User

      User - GRAYBERUSER1
      Risk Id - F00102501
      Mitigating Reference No. - MCFI0002
      Valid From - 02/16/2005
      Valid To - 10/16/2005
      Monitor - Jack Foster

```

Critical Transactions Reports

Table 7-2: Types of Critical Transaction Reports

Critical Transactions - User - Technical Summary
Critical Transactions - User - Technical Detail
Critical Transactions - User - Business Summary
Critical Transactions - User - Business Detail
Critical Transactions - Role - Technical Summary
Critical Transactions - Role - Business Summary
Critical Transactions - Profiles - Technical Summar
Critical Transactions - Profiles - Business Summary
Critical Transactions - HR Objects - Technical Summary
Critical Transactions - HR Objects - Technical Detai
Critical Transactions - HR Objects - Business Summary
Critical Transactions - HR Objects - Business Detail

Critical Roles and Profiles Reports

Table 7-3: Types of Roles and Profiles Reports

Critical Roles/Profiles - User - Technical Summary
Critical Roles/Profiles - User - Business Summary
Critical Roles/Profiles - Roles - Technical Summary
Critical Roles/Profiles - Roles - Business Summary
Critical Roles/Profiles - Profiles - Technical Summary
Critical Roles/Profiles - Profiles - Business Summary
Critical Roles/Profiles - HR Objects - Technical Summary
Critical Roles/Profiles - HR Objects - Business Summary

Mitigation Controls Reports

Table 7-4: Types of Mitigation Controls Reports

Mitigation Controls - User - Technical Summary
Mitigation Controls - User - Business Summary
Mitigation Controls - Role - Technical Summary
Mitigation Controls - Role - Business Summary
Mitigation Controls - Profile - Technical Summary
Mitigation Controls - Profile - Business Summary
Mitigation Controls - HR Objects - Technical Summary
Mitigation Controls - HR Objects - Business Summary

Simulation Reports

Simulation reports are generated by selecting values in the Risk Analysis control panel and clicking the Simulation button.

- You can simulate adding single Roles to a composite Role. Specify the composite Role or range of composite Roles in the Risk Analysis control panel and specify the single Role or range of single Roles in the Simulation form.
- You can use the User Assignment button to assign Roles or Profiles that do not produce a SoD.

Table 7-5: Types of Simulation Reports

User-Based Simulation Report - Technical Summary View
User-Based Simulation Report - Technical Summary View
User-Based Simulation Report - Business Summary View
User-Based Simulation Report - Business Summary
User-Based Simulation Report - Executive Summary

Background Reports

Background reporting allows reports to be generated for large numbers of Users, Roles, Profiles, or HR Objects. All procedures for running background reports are the same as when executing reports in the foreground. The only difference is the report formats. You can use SM37 or SU01 to view the generated background reports.

You can run the analysis in background by specifying all your selections in the Risk Analysis control panel and the clicking Run in Background on the Compliance Calibrator menu. See section 4.10, Running Risk Analyses in Background Mode for more information.

CAUTION: If you are running a Risk Analysis as a background job for a large number of Users, Roles, or Profiles that may have many SoDs, make certain you have the Configuration Option Multiple Spool Option set to YES to avoid any memory errors.

Figure 7–5: Example of a Background User-based SoD Transaction Code Level Report

Statistics	Number of
Records passed	23,956

IDENTIFICATION INFORMATION					
ID:	JAVILAN	Date:	01/24/2005	Time:	18:57:04
System:	V05	Client No.:	100		

Action Parameters:	User Based Analysis
SCR ID:	SCR_S00_05
Group:	
Level:	ALL
Type of report:	SoD at Transaction Code Level
Print Format:	Detail Report
Job Number:	
Type:	AT1
Job ID:	LOCAL
Total number of Conflicts:	3,309

Offending Transaction	Role/Profile Description	Risk Description	Level	Mitigating Control	Monitor	S
SCR ID: SCR_S00_05	NAME: TEST FIFTH USER	USER GROUP: VIRSCGP1				
Invoice Contract (VX42)	SCR_S00_001: TEST CROSS SYSTEM DESCRIPTION AND FOR MAXIMUM CHARACTER LEN	S003224: Maintain fictitious customer and initiate orders	High			L
Invoice Customer (Sales) (VD02)	SCR_S00_001: TEST CROSS SYSTEM DESCRIPTION AND FOR MAXIMUM CHARACTER LEN	S003224: Maintain fictitious customer and initiate orders	High			L

Management Reports

The Management Reports is located in the VIS menu. This report displays information about authorization objects for Users, Roles, Profiles, or HR Objects.

In order to generate this report you must specify Users, Roles, or Profiles in the Risk Analysis control panel and choose the SoD at Authorization Object Level report type.

- This report displays the first and last names of users for User-based analysis and a Role Description for Role-based analysis.

Figure 7-6: User-based Management Reports from the VIS menu

Run By: JAVILAN		Time: 14:48:08
Selection Parameters		
User:	CONT1000 to CONT3000	
User Group:		
Risk Level:	ALL	
Type of Report:	SOD at Authorization Object Level	
Report Format:	Summary Report	
Group Number:	All	
User Type:	All	
Ignore:	None	
Violations Count		
Total Number of Violations:	169	
Total Number of Users with Violations:	3	
Report Summary		
Risk Description	Risk Level	Number of Users
B001:Basis Development & System Administration	Medium	1
B002:Basis Development & Configuration	High	1
B003:Basis Development & Client Administration	Medium	1
B004:Basis Development & Transport Administration	High	1
Risk Violations		
User Id: CONT1000	Name: Mark Smith	User Group: MM-GLOBAL
Risk Description	Risk Level	
M006:Receive/issue incorrect amount and adjust via MM stock count	High	
User Id: CONT2000	Name: Steffi Jones	User Group: AP-GLOBAL
Risk Description	Risk Level	
F001:Maintain fictitious GL account & hide activity via postings	Medium	
F005:Maintain bank account and post a payment from it	High	
F022:Maintain fictitious GL account & hide activity via currency or tax postings	Medium	
User Id: CONT3000	Name: Matt Foreman	User Group: SECURITY-GST
Risk Description	Risk Level	
B001:Basis Development & System Administration	Medium	

Analytical Report

The Analytical Report is located in the VIS menu. This report displays information about authorization objects for Roles.

In order to generate this report you must specify a Role or range of Roles in the Risk Analysis control panel and choose the SoD at Authorization Object Level report type.

NOTE: This report can only be generated in background mode. A full Role scan is performed before the results are reported and longer run-times should be expected.

Figure 7-7: Role-based Analytical Report from the VIS menu

ANALYTICAL REPORT		
General Information		
Report Type:	Role Based	System: R46 100
Analysis Type:	SoD at Authorization Object Level	Date: 03/07/2005
Run By:	JAVILAN	Time: 14:57:33
Selection Parameters		
Role:	VA*	
Risk Level:	ALL	
Type of Report:	SoD at Authorization Object Level	
Report Format:	Summary Report	
Group Number:	All	
Ignore:	Expired Users	
Risk Violations		
Role: VAP006:PROC_DOWN_PAY>000-MODL Name: AP: Process Down Payment - Model		
No of Conflicts in the Role:	3	No of Users assigned to the Role: 1
Risk Description		Risk Level
F001: Maintain fictitious GL account & hide activity via postings		Medium
F005: Maintain bank account and post a payment from it		High
F022: Maintain fictitious GL account & hide activity via currency or tax postings		Medium
Role: VAP011:GEN_PROCESSOR>000-MODL Name: AP: General Processor Role - Global		
No of Conflicts in the Role:	4	No of Users assigned to the Role: 1
Risk Description		Risk Level
F001: Maintain fictitious GL account & hide activity via postings		Medium
F022: Maintain fictitious GL account & hide activity via currency or tax postings		Medium
P003: Create fictitious vendor invoice and initiate payment for it		High
P052: Create fictitious vendor invoice and initiate manual checks for it		High

Invalid Mitigating Controls Report

This report is located in the Utilities menu. This report addresses invalid Mitigation Controls for Users. The report must be run at both the Tcode and Object level to report the appropriate User Mitigating Controls.

The Invalid Mitigating Controls report is used to identify two types of invalid controls -

- Mitigation Controls due to expire by a specified date
 - Mitigation Controls no longer valid, because Roles are no longer assigned to the User, or because of changes to assigned Roles
- The report is run based on values entered in the Risk Analysis control panel -
- Select a User or range of Users
 - Choose to run the report at SoD Transaction Level or SoD Authorization Object Level
 - The report is available in Summary Format only

Once you click on Invalid Mitigation Controls in the Utilities menu, a dialog box is displayed so you can specify the Validation Date. Any Mitigation Controls expiring before this date for the selected Users are included in the report. The generated report lists the invalid Mitigation Control records from the Mitigated User table based on the specified date.

After the date is entered a pop box will provide an option to run this job in background. Click YES to run the report in the background, or click NO to run the job in the foreground. The first step of this job retrieves records from the Mitigated User table for the specified date and checks if there are Users satisfying those entries or not. Since a User scan is performed, this job could have an extended run time. Therefore, it is recommended you run generate the report in the background.

Figure 7–8: User Invalid Mitigation Control Report

Data statistics		Number of			
Records passed		4			

SOD Group ID	User/Role Name	User Group	MC Valid From Date	MC Valid To Date	Mit Ref. No.
0014	SCU_SOD_03	VIRSC6P1	08/14/2003	09/04/2005	MC0005
0014	SCU_SOD_07	VIRSC6P1	08/14/2003	09/05/2005	MC0003
F007	SCU_SOD_05	VIRSC6P1			
M002	SCU_SOD_08	VIRSC6P2	08/14/2001	09/03/2003	MC0004

8. Tool Box Reports and Utilities

Introduction

NOTE: All reports and utilities in the Virsa Tool Box are assigned authorization groups. This means that a User needs authorization for object S_PROGRAM to execute the report. Refer to the SAP Compliance Calibrator by Virsa Systems Security Authorizations Guide for more information.

Rule Architect Reports and Utilities

Authorization Object by Roles/Profiles Report (not in SoD Tables)

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > SOD / Audit Utilities & Reports

This utility produces a report listing all the authorization objects for the specified Roles and Profiles not included in any SoD table.

Once you have generated the report you can mark the objects as analyzed and valid for exclusion from the SoD tables. Place a checkmark next to each object and then click Update. To view the marked objects run the report again and click Analyzed Auth Obj instead of the Execute button.

Comparing Critical Transaction Matrices

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > SOD / Audit Utilities & Reports

This utility uses the existing Critical Transaction table in Compliance Calibrator Rule Architect as the master data table and compares it to a tab-delimited text file using the same format as the master data table. The resulting report displays any transactions in the text file that do not exist in the master data table. Only the transaction code is used for comparison. The values in other fields are ignored.

You can also upload the missing rules from the text file to the master data table from the report.

Figure 8-1: Comparing Critical Transaction Matrices Report

Check	Transaction	Risk Id	Risk Description	Risk Level	Status
<input checked="" type="checkbox"/>	F-67	1	Arch	Medium	Enable
<input type="checkbox"/>	MM01	al m		Critical	Enable
<input type="checkbox"/>	MM02	all		Critical	Enable
<input type="checkbox"/>	SCC4	Clie	F008	Medium	Enable
<input type="checkbox"/>	SCC6	Clie	F010	Medium	Enable
<input type="checkbox"/>	SE11	Data	F015	High	Enable
<input type="checkbox"/>	SE38	ABAP	F001	High	Enable
<input type="checkbox"/>	SM50	Work	K006	Medium	Enable
<input type="checkbox"/>	SUGR	This	RR01	Critical	Enable

Comparing SoD Authorization Objects

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > SOD / Audit Utilities & Reports

This utility uses the existing Authorization Objects Rules table in Compliance Calibrator Rule Architect as the master data table and compares it to a tab-delimited text file using the same format as the master data table. The resulting report displays any Rules in the text file that do not exist in the master data table. Only the authorization objects "Field", "From", and "To" fields are compared. The values in other fields are ignored.

You can also upload the missing rules from the text file to the master data table from the report.

Optimizer for SoD Data Table

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > SOD / Audit Utilities & Reports

This utility is used to optimize field values with an OR operand in any authorization object.

Rules Table After Optimization

The optimized Rules table is saved to a text file on your desktop.

CAUTION: It is recommended that you NOT upload the created Transaction Code Rules file. Doing this will invalidate Rule Architect's Risk and Function organization. It is recommended you use the data in the deleted objects file to edit the appropriate Risks and Functions through Rule Architect.

Comparing Different SoD Matrices

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > SOD / Audit Utilities & Reports

This utility uses the existing authorization object rules in Compliance Calibrator as the master data table and compares it to a tab-delimited text file. The resulting report displays any rules in the text file that do not exist in the master data table. The fields used for comparison are "Field", "From", and "To". Any differences in other field values are ignored.

You can also upload the missing rules from the text file to the master data table from the report. Checkmark the Rules you want to upload and click Update.

SoD Rule Validation Tool

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > SOD / Audit Utilities & Reports

If you have included the same transactions in two different Risks duplicate Rules are created. This report validates the data for duplicate Rules and creates two files, one with all the valid data and the other with duplicate data. This report accepts SOD Tcode data by means of an external file or Compliance Calibrator SOD Tcode table.

Field Definitions

- Upload Data, External File - If you want to check a set of Rules stored in an external file you can use these fields to specify the file's location.

E.G. if you use a Matrix Rules tables to store Rule sets you can download the all the Rules and save it as a tab-delimited text file.

NOTE: If you are checking an external file for duplicates the file must be in the same format as the SOD Tcode table and saved as tab-delimited text file.

- Compliance Calibrator SoD TCode Table - Choose this option to check the standard (Global) transaction level Rules table for duplicates.
- Files for Download, Valid Data - Specify the full pathname of the file you want the utility to store the Rule set after checking for duplicates. This is a required field.
- Files for Download, Duplicate Data - Specify the full pathname of the file you want the utility to store the duplicate Rules. This is a required field.

CAUTION: It is recommended that you NOT upload the created Transaction Code Rules file. Doing this will invalidate Rule Architect's Risk and Function organization. It is recommended you use the data in the deleted objects file to edit the appropriate Risks and Functions through Rule Architect.

Non Reference Report

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > SOD / Audit Utilities & Reports

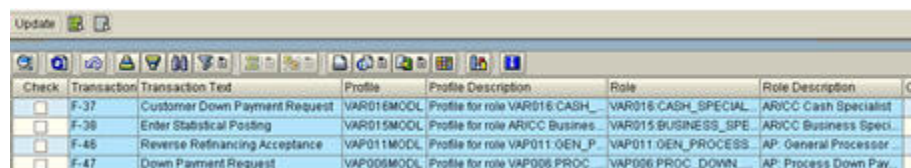
This report is used to identify transactions in Roles or Profiles not included in the Compliance Calibrator Rules table.

Enter the Roles and Profiles you want to examine and click Execute.

Once you have generated the Non Reference Report you can checkmark each reported transaction by clicking the checkbox and then clicking Update. This moves the marked transaction to the Analyzed TCodes table. Transactions listed in the Analyzed TCodes table are not included the next time you generate the report for the same Roles and Profiles.

You can view analyzed tcodes by clicking the Analyzed TCodes button.

Figure 7 13, Non Reference Report



Check	Transaction	Transaction Text	Profile	Profile Description	Role	Role Description	Co
<input type="checkbox"/>	F-37	Customer Down Payment Request	VAR016MODL	Profile for role VAR016:CASH_	VAR016:CASH_SPECIAL	ARICC Cash Specialist	
<input type="checkbox"/>	F-38	Enter Statistical Posting	VAR015MODL	Profile for role ARICC Business	VAR015:BUSINESS_SPE	ARICC Business Speci	
<input type="checkbox"/>	F-45	Reverse Refinancing Acceptance	VAP011MODL	Profile for role VAP011:GEN_P	VAP011:GEN_PROCESS	AP: General Processor	
<input type="checkbox"/>	F-47	Down Payment Request	VAP006MODL	Profile for role VAP006:PROC_	VAP006:PROC_DOWN	AP: Process Down Pay	

TCodes by Roles/Profiles Never Executed in a Specific Time Period

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > SOD / Audit Utilities & Reports

This report displays a list of transactions not used within the specified time period.

When you execute the utility, it analyzes the transactions in the selected Roles and Profiles. If any transactions are found that were never executed in the given time period, they are included in the report.

Field Definitions

- Transaction Monitor Time Frame - The From and To fields have a pop-up menu displaying the last three months, e.g. 1/2005, 2/2005, 3/2005. Choose the time period you want to analyze.
- Table Query Time Frame - These fields are filled in automatically
- Enter File Name for Upload - To use an external file, you must run the utility Monitor actual usage of Conflicting and Critical Transactions. This utility produces a tab-delimited text file listing all the transactions executed within a given time period. You can use this file to determine what transactions have not been executed for the specified Roles or Profiles.

Maintain ORGUSERS Table

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > Miscellaneous

The table created and maintained with this utility is used in combination with the Organizational Rules table. See 1.17, Defining and Maintaining Organizational Rules for more information.

Best practice is to schedule this utility to run in the background on a nightly basis (see below)

- By specifying a range of users and clicking the Execute button the ORGUSERS table is updated and the users and their Organizational Level field values and Organizational Value field values are added to the table. If you don't specify a range of Users all Users are analyzed. This field is optional.
- If you specify an Organizational Level, e.g. BUKRS, only those users matching that parameter value are added to the ORGUSERS table. This field is optional.
- If you specify an Organizational Value, only those users matching that value are added to the ORGUSERS table. If you include a value in this field you must also include a value in the Organizational Level field. This field is optional.
- If you check Test Only a list of users matching your criteria are displayed, but are not added to the ORGUSERS table.

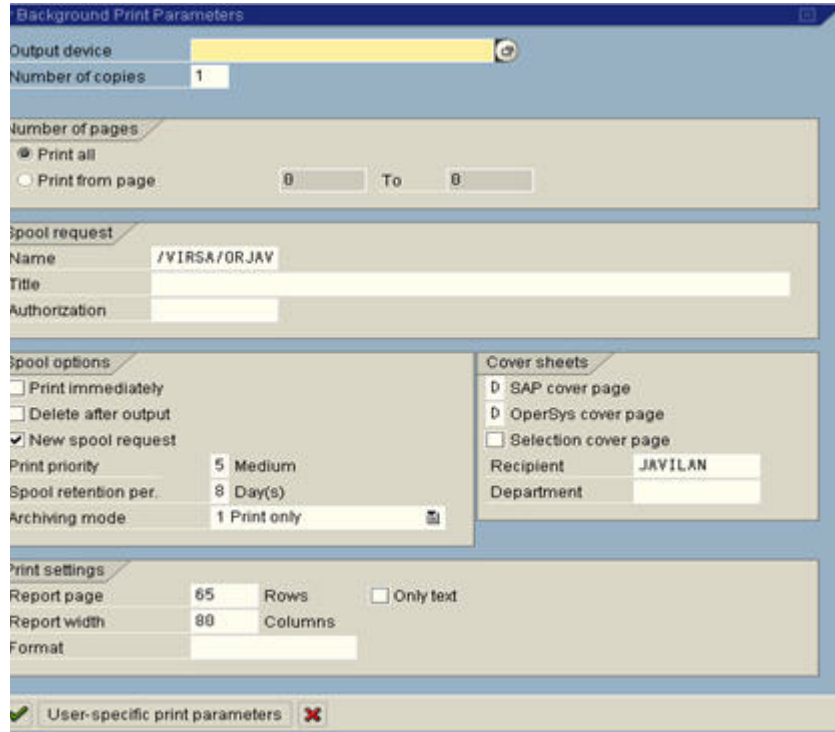
When this utility is executed it first checks the records in the Organizational Rules table. Each record in the Organizational Rules table specifies an Organizational Level and field values for that Level. Only those Users matching any of the Organizational Levels and their corresponding field values are added to the ORGUSERS table.

NOTE: Only the Organizational Rules set to "Enabled" are checked.

Scheduling a Background Job

You can schedule a background job to run this utility nightly to maintain the ORGUSERS table. Use the following process to schedule the background job -

1. From the Maintain ORGUSERS Table utility screen click the Program menu and then click Execute in Background.

Figure 8–2: Scheduling a Background Job for the ORGUSERS Table


2. Enter a default printer and click Execute.
Make sure New Spool Request is checked and Print Immediately is unchecked.
3. Click Date/Time and schedule the Start Date and Time.
4. Click Period Values to specify running the job daily.
5. Click Save to save your job.

You can view your job using SM37.

Mitigation Control Reports

Where Used List for Mitigating Control Reference Monitor

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > Miscellaneous

This report lists which Users, Roles, Profiles, or HR Objects have the specified Mitigation Controls assigned.

Figure 8–3: Where Used List for Mitigating Control Reference/Monitor Report

Where Used List for Mitigating Control Id / Monitor						
Group	User	MC Valid From	MC Valid To	Ref.No.	Monitoring Person	Status
05	CONT2000	12/27/2004	05/21/2005	MCFI0001	EMPL4500	End
There are no records in the Mitigating Control for Role Table.						
There are no records in the Mitigating Control for Profile Table.						
There are no records in the Mitigating Control for HR Object Table.						

Alerts Module Utilities

Activity Monitoring

This utility can be found in the Tool Box in the following location -

Virsa Utilities & Reports > Monitoring

This utility builds the log files used to generate Alerts. Activity Monitoring should be set up as a background job to run automatically. The job (SM37) generates the Transaction Log and the Alerts module uses the Log to create alerts. Since the job runs in the background on a periodic basis there is no need to use this utility unless you want to generate alerts before the next scheduled job.

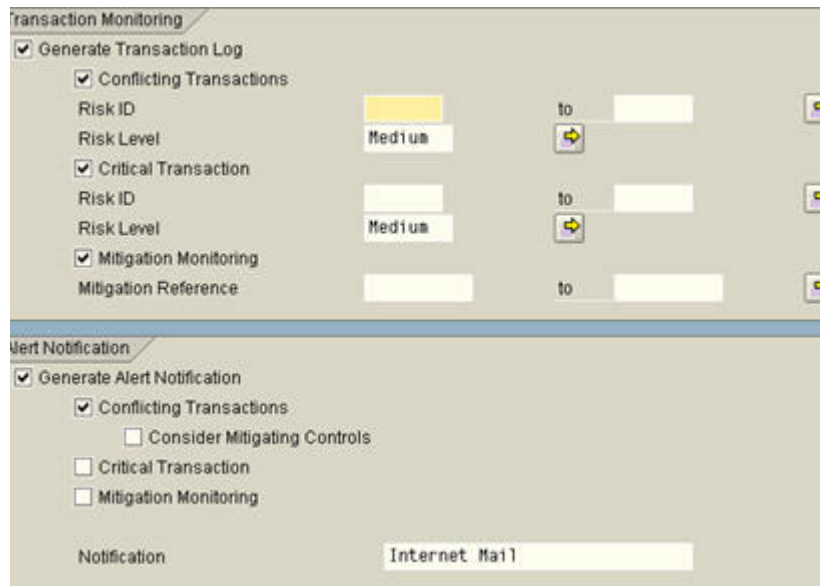
There are two activities related to this utility; generating the Transaction Log, which is used to collect data for Alerts, and generating the Alerts.

If you checkmark Generate Transaction Log and don't checkmark Generate Alert Notification, the Log is updated, but no new Alerts are displayed in the Alerts module screen.

Field Definitions

- **Transaction Monitoring** - You must checkmark Generate Transaction Log to update the Transaction Log. The Log is updated according to the data chosen -
 - **Conflicting Transactions** - You must checkmark to include these transactions in the Log. You can filter the transactions added by specifying a Risk ID and/or a Risk Level. Wildcards can be used to specify Risk IDs.
 - **Critical Transaction** - The process for updating the Log with Critical transactions is the same as Conflicting transactions.
 - **Mitigation Monitoring** - You must checkmark to include in the Transaction Log. Mitigation Monitor Alerts are generated when the transactions specified in the Reports tab of a Mitigation Control definition form have not been executed with the Frequency period (also specified on the Reports tab).
- **Alert Notification** - You must checkmark Generate Alert Notification for Alerts to be generated based on Transaction Log data.
 - **Conflicting Transactions** - Checkmarking this box displays Conflicting transaction Alerts based on the data in the latest Transaction Log. If you checkmark Consider Mitigating Controls, mitigated SoDs are not included.
 - **Notification** - You can specify either SAP mail or Internet Mail. This determines how Alerts are emailed to the Monitors listed in the Alerts Module Email Configuration table.

NOTE: You must make sure the Monitors listed in the Configuration table are able to receive internet mail.

Figure 8–4: Activity Monitoring Form


Transaction Monitoring

☒ Generate Transaction Log

☒ Conflicting Transactions

Risk ID: to

Risk Level: to

☒ Critical Transaction

Risk ID: to

Risk Level: to

☒ Mitigation Monitoring

Mitigation Reference: to

Alert Notification

☒ Generate Alert Notification

☒ Conflicting Transactions

☐ Consider Mitigating Controls

☐ Critical Transaction

☐ Mitigation Monitoring

Notification:

Scheduling a Background Job

You can schedule a background job to run this utility nightly to maintain the Alerts Transaction Log table. Use the following process to schedule the background job -

1. From the Activity Monitoring utility screen click the Program menu and then click Execute in Background.
2. Enter a default printer and click Execute. Make sure New Spool Request is checked and Click Date/Time and schedule the Start Date and Time.
3. Click Period Values to specify running the job daily.
4. Click Save to save your job. You can view your job using SM37.

Risk Analysis Reports

User Access Report

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > User Administration Utilities and Reports

The report generated by this utility displays two sets of data -

- SoDs at Authorization Object level - The report lists SoD violations by Risk ID for the selected Users or User Groups, or all Users within a Department.
- Critical Objects - The report also lists access to any objects stored in the Critical Objects table.

Figure 8–5: User Access Report Form

The screenshot shows the 'User Access Report Form' with the following settings:

- Select the type of Analysis:** ☒ User, ☐ User Group, ☐ Department. Range: Cont1000 to []
- Select Risk Level for Analysis:** ☐ Critical, ☐ High, ☐ Medium, ☐ Low, ☒ All
- Report Format:** ☒ Summary Report, ☐ Detail Report
- User Type:** ☐ Dialog, ☐ Communication, ☐ System, ☐ Service, ☐ Reference, ☒ All
- Exclusions:** ☐ Locked Users, ☐ Expired Users, ☐ Mitigating Controls, ☒ Expired Roles
- Rules Template:** Object Rules Template: GLOBAL

Maintaining the Critical Objects Table

You can add records to the Critical Objects table through Compliance Calibrator, or you can upload the data from a tab-delimited text file. The file must be in the same format as the table. The table contains three columns of information, Object, Risk Description, and Enable/Disable. Only those records with an Enable status are used during report generation.

Figure 8–6: User Access Report Output

Report Run By:

JAVILAN

Date:

03/17/2005

Time:

18:32:18

Item:

V05

Event No.:

100

User ID:

JAVILAN

User Group:

Department:

User Name:

Javilan Jake

User Validity End Date:

ID	Role Description
SC_GLBL_GENERAL_ACCESS	Basic access for Demo system
S_TCODE	Transaction Authorization
CA_ADMINISTRATOR	Compliance Calibrator Administrator
S_TCODE	Transaction Authorization
CA_ADMINISTRATOR_OLD	Compliance Calibrator Administrator - All Access
CAAT_ADMINISTRATOR	Role for Administrator with full access
S_TCODE	Transaction Authorization

Risk ID

Monitor

Risk Description

R001

Basis Development & System Administration

R002

Basis Development & Configuration

R003

Basis Development & Client Administration

R004

Basis Development & Transport Administration

Analysis of Called Transactions in Custom Code

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > SOD / Audit Utilities & Reports

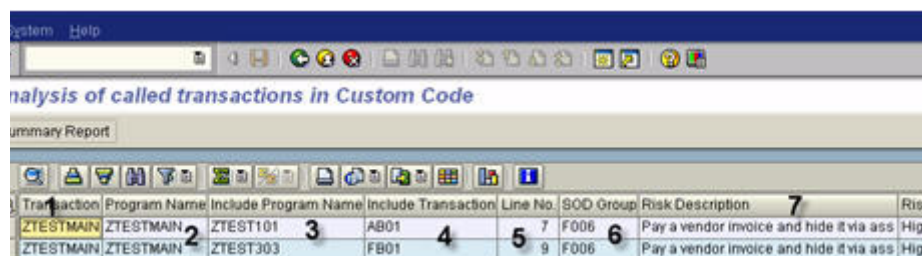
This report is used to analyze conflicts in custom transactions due to SAP native transactions in the custom code. You can use the information in the report to update your Rule Architect Functions to include the identified custom transactions. If transactions appearing in the Transaction column are not included in your Functions, no Rules are generated for the transaction.

Checking Any TCodes in SoD Conflicts limits the report results to conflicting transactions.

Figure 8–7: Summary Analysis of Called Transactions

Transaction	SOD	SOD Group	Risk Description	Risk Level
TESTMAIN	AB01,FB01	F006	Pay a vendor invoice and hide it via ass	High
TESTMAIN	FD05,VA01	S003	Maintain fictitious customer and initiat	High
TESTMAIN	FD05,FB01	S004	Change customer-master and enter inappro	High

Figure 8–8: Detailed Analysis of Called Transactions

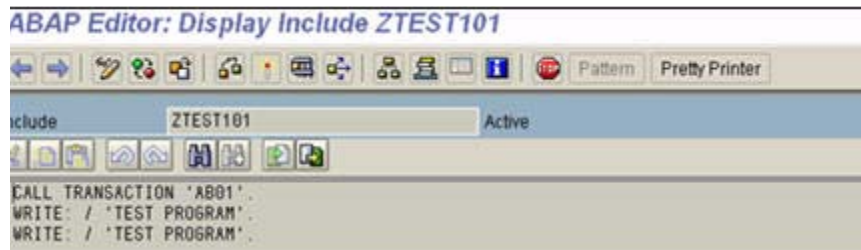


Transaction	Program Name	Include Program Name	Include Transaction	Line No.	SOD Group	Risk Description	Risk Level
ZTESTMAIN	ZTESTMAIN	ZTEST101	AB01	7	F006	Pay a vendor invoice and hide it via ass	High
ZTESTMAIN	ZTESTMAIN	ZTEST303	FB01	9	F006	Pay a vendor invoice and hide it via ass	High

1. Transaction
2. Program for Transaction
3. Include Program Name (if any)
4. Transaction that is being called either in include program (if 3 appears) else this transaction is being called in main program
5. Line No. called from code
6. SOD Group ID
7. Risk Description
8. Risk Level

Double Click on Include Transaction (AB01) and report as show below will be displayed. This report explains in detail where the transaction was called in the custom code.

Figure 7 30, Display Custom Code



ABAP Editor: Display Include ZTEST101

include ZTEST101 Active

```
CALL TRANSACTION 'AB01'.
WRITE: / 'TEST PROGRAM'.
WRITE: / 'TEST PROGRAM'.
```

Management Report for SoD Remediation

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > Management Level Reports

This utility generates a list of Risks for the specified Users or User Groups. The conflicting transactions and the Roles they are associated with are identified. You can filter the report by entering a specific Risk ID in the Group ID field, and by selecting the Risk Level for analysis.

Monitor Actual Usage of Conflicting & Critical Transactions

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > SOD / Audit Utilities & Reports > Monitoring & Analysis of Transactions Actually Executed By Users

This utility produces an extract data file and then uses the file to generate the Actual Usage report. All Users are included in the extract file. Each time you run the extraction process the new data is appended to the file.

The report lists the conflicting and critical transactions used by the specified Users within the time period specified.

NOTE: The extract file can be used when running the utility, TCodes by Roles/Profiles Never Executed.

Processing Field Definitions

- Start Time - Specify the time of day to begin collecting data
- Date - Specify the date to extract the data
- Read Time - This field specifies the amount of time to add or subtract to the Start Time. If the Start Time is left at 00:00:00, Compliance Calibrator assumes the present time, subtracts the amount of time specified in the Read Time field, and extracts data for that time period. If the Start Time contains a non-zero time value, the value in the Start Time field is added, and extracts data for that time period.

Select the Type of Analysis Field Definitions

- Period - This is a date field. The extract data file generated above may contain many days of transaction data. You can limit the report results using this field.
- Group Number - This field accepts Risk ID values. You can limit the report results by limiting the Risk IDs analyzed.

Managements Reports

This report is located on the Compliance Calibrator toolbar instead of in the Tool Box.

The report displays a snapshot of statistical information about Risk Analyses, Rules, and Mitigation Controls. The statistics included in the report are time-based and you can specify the time period to generate different report data.

NOTE: This statistics in this report are based on background jobs. Foreground Risk Analyses are not included in the statistics.

Figure 8–9: Compliance Calibrator Management Reports

User Summary		Role Summary	
Number of Users Analyzed	30	Number of Roles Analyzed	
Number of Mitigated Users	0	Number of Mitigated Roles	
Number of Users Ignored	0		
User Analysis		Role Analysis	
Number of Violations	80367	Number of Violations	
Critical Risk Level Violations	0	Critical Risk Level Violations	
High Risk Level Violations	63792	High Risk Level Violations	
Number of Users with Violations	18	Number of Roles with Violations	
Number of Mitigated Users	0	Number of Mitigated Roles	
Number of Mitigated Violations	0	Number of Mitigated Violations	
SOD Rule Summary		SOD Rule by Business Process	
Number of Active Rules	5357	Basis	
Number of Disabled Rules	13392	Finance	
Critical Risk Level Rules	0	HR and Payroll	
High Risk Level Rules	4252	Materials Management	
Number of Risks	21	Procure to Pay	
Number of Functions	0	Order to Cash	
Mitigating Controls		Mitigating Controls by Business Unit	
Number of Active Controls	1	Corporate Finance	
Valid Mitigating Controls	1		
Critical Risk Level Controls	0		
High Risk Level Controls	756		
Mitigating Controls without Monitor	0		
Critical Transactions and Roles		User Group Violations	
Number of Active Critical Transactions	312		
Number of Disabled Critical Transactions	0	SUPER	
Number of Active Critical Roles	0		
Number of Disabled Critical Roles	0		
Number of Active Critical Profiles	7		
Number of Disabled Critical Profiles	0		

Count Authorizations for Users

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > User Administration Utilities and Reports

This report lists the number of authorizations for a User. The report below Lists Counts Per Role/Profile.

Field Definitions

- User ID - Specify the User or range of Users to be analyzed.
- Count Limit - The numeric value you enter limits the number of Roles displayed for each User.
- List Counts Per Role/Profile - Includes the number of authorizations for each Role listed in the report

Figure 8–10: Count Authorizations for User Report

Report Run By: JAVILAN		
Date: 02/17/2005		
Time: 16:09:03		
System: R46		
Client No.: 100		
User	Role/Profile Name	Number of Authorization
JONT1000	YMM003:MMGENADISP>000-ENTR	140
JONT1000	YMM012:SMGDS_RECEIPT>000-MODL	35
JONT1000	VUS001:BASIC_PRD_USR>000-ENTR	26
JONT1000	Total No. Of Authorizations:	201
	System Limit:	0

Count Authorizations in Roles

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > Role/Profile Administration Utilities and Reports

This report displays the number of authorizations for each Role included in the report.

Figure 8–11: Count Authorizations for Roles Report

Report Run By: JAVILAN	
Date: 02/17/2005	
Time: 16:40:38	
System: R46	
Client No.: 100	
Role Name	No. of authorizations
VAP006:PROC_DOWN_PAY>000-MODL	9
VAP011:GEN_PROCESSOR>000-MODL	42
VAP014:NETTING_AP&AR>000-MODL	8
VAR015:BUSINESS_SPEC>000-MODL	54
VAR016:CASH_SPECIALIS>000-MODL	29
Total No. of Roles	5
Average Authorizations Per Role	28

Display Changes to Profiles

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > Role/Profile Administration Utilities and Reports

This report displays any changes to a Profile within a specified time period.

Security and Controls Policies and Procedures

This report can be found in the Tool Box in the following location -

Custom Utilities and Reports

This utility is used to generate the Security Policy document.

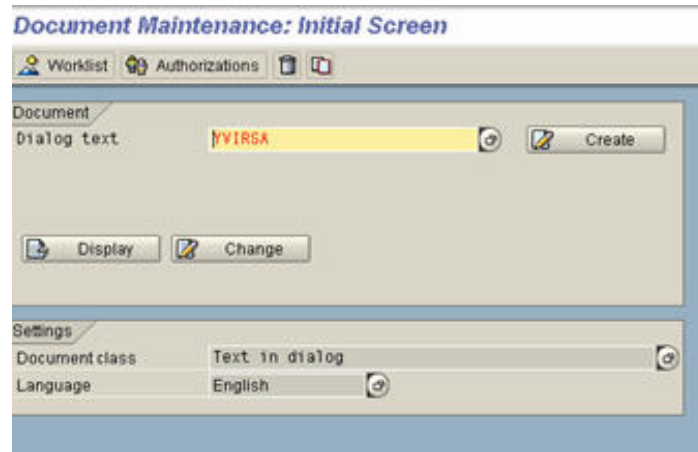
The information to be documented in the Security Policy Document must be provided to a developer to create the Dialog Text.

Development access will be required to create the Text. Use the following procedure to create the Security Policy document.

Creating the Security Policy Document

1. In the Compliance Calibrator Toolbox control panel type transaction /OSE61.
2. In Document Class field, select "Text in dialog"
3. Give a name in the Dialog text. (ex: YVIRSA)
The name may be up to 20 characters
4. Click Create.
Type the security documentation using the SAP text standard functionality.
5. Click Save and Generate.

Figure 8–12: Document Maintenance Table



Specify the Security Policy Document Text

1. Open the Configuration Options screen from the Compliance Calibrator menu.
2. Click New Entries.
3. Select Security and Control Policies and Procedures
4. Type the name of the Dialog Text created in the previous process.
5. Click Save.

Viewing the Security Policy Document

You can use the Tool Box utility, Security & Controls Policies and Procedures to view the created file.

Expired and Expiring Roles for Users

This report can be found in the Tool Box in the following location -

Virsa Utilities and Reports > User Administration Utilities and Reports

This report lists all expired or expiring Roles for the specified Users.

Field Definitions

- **Expiry Date** - This field specifies the target date to search for expiring Roles. If you specify a range of dates, all Roles expiring within the date range are included in the report.
- **Expired Roles** - The Expired Roles report uses the current date to search for expired Roles. The Expiry Date does not affect this report.
- **Expiring Roles** - The Expiring Roles report must have at least one date specified in the Expiry Date field. If you Role types in the report, Expired Roles are displayed in red.
- **Display Direct Assigned Role** - Checking this option displays the individual Roles assigned to a User. Composite Roles are included in the report as a single line item.

Maintenance Utilities

Compliance Calibrator Data Maintenance

This report can be found in the Tool Box in the following location if you are using SAP Compliance Calibrator by Virsa Systems version 4.6c or higher. This utility is not available in SAP Compliance Calibrator by Virsa Systems version 4.6b.-

Virsa Utilities & Reports > SOD / Audit Utilities & Reports

This utility displays the data stored in each table.

NOTE: In order to display the SoD Transaction Code table and SoD Authorization Objects table the Configuration Option Rule Architect Activation must be set to "NO".

Rule Architect Wizard

This utility can be found in the Tool Box in the following location -

Virsa Utilities & Reports > SOD / Audit Utilities & Reports > Virsa SOD Rule Builder

The Rule Architect Wizard leads you through a five-step process to build your transaction level and authorization object level Rules tables. Click the Execute button to start the wizard.

Compliance Calibrator's Rule Architect uses Functions to group business-related transactions. Functions with conflicting transactions are then associated with a Risk. Risks are then used to generate transaction code level and authorization object level Rules based on the pairs of conflicting transactions.

When you run the wizard predefined Risk and Function data, as well as the relationships between them and transactions and objects is first uploaded from predefined text data files delivered with Compliance Calibrator.

Compliance Calibrator compares SU24 objects with the predefined object set and displays any mismatched objects. You can then choose to include those objects during Rule creation.

Overview

The following points outline the tasks you must perform or the steps taken by the conversion wizard.

- **Prepare the data files delivered with Compliance Calibrator 4.0** - The tab-delimited text files contain the standard default information used to define Rule Architect constructs - Business Processes, Risks, and Functions. The files also define the relationships between these constructs and transactions and authorization objects; e.g. which transactions and authorization objects are associated with each Function, and which Functions are associated with each Risk ID. These constructs and their associations are then used to generate the Virsa Rule tables for transactions and authorization objects.

These files may be edited to change the default information, e.g. you can add, remove, or change the Business Processes defined in the `business_processes.txt` data file; you can also disable any transaction associated with a Function, or disable any Risk. By disabling a transaction

or Risk you prevent those transactions and Risks from being used during Rules generation.

- Step One, Rule Architect Activation - The first step the wizard performs is to check the status of the Rule Architect Activation Configuration Option. This option's value must be set to YES for the conversion process to begin.
- Step Two, Specify the location of the data files - The conversion wizard needs to know what directory on the server holds the data files.
- Step Three, Check for coupled transactions - The wizard checks for custom (Z) transactions. During this step you can decide which coupled transactions are included, and are used during Rules generation.

NOTE: The Coupled Transaction feature is not available in SAP Compliance Calibrator by Virsa Systems version 4.6b.

- Step Four, Assigning Objects - This step presents two tables from which you'll choose what objects to include when generating your new Rule sets.
 - Predefined Virsa Objects - This table displays all the predefined Functions and their associated transactions and objects.
 - Custom Objects - This table displays all your objects and their values that have not been included in the predefined set of objects.
- Step Five, Generate New Rules - The wizard performs this step automatically based on the choices you made in the previous steps.

Preparing the Predefined Rule Architect Data Files

There are six tab-delimited text files delivered to you with the Compliance Calibrator transport files. These files contain the table data used to generate your Transaction Level and Authorization Object Level Rules tables. The Rules generated from data in these tables are the pre-defined Virsa Rules set.

- business_process.txt - This file lists the standard Business Process IDs and their descriptions. Business Process IDs are assigned to help organize your Risks and Functions.
- function.txt - This file lists the standard Functions IDs and their descriptions. Functions are used to organize groups of transactions.
- function_bp.txt - This file associates Function IDs and Business Process IDs. The columns in this file contain the following information:
 - Column One - Function ID
 - Column Two - Business Process ID
- function_object.txt - This file associates Function IDs with transaction codes and their objects and objects values.
- function_tcode.txt - This file associates Function IDs with transaction codes. The columns in this file contain the following information:
 - Column One - Function ID
 - Column Two - Transaction Code
 - Column Three - Transaction Status (0 = Enabled, 1 = Disabled)
- risks.txt - This file describes each Risk. The columns in this file contain the following Risk information -
 - Column One - Risk ID
 - Column Two through Six - Function IDs associated with the Risk ID
 - Column Seven - Business Process ID associated with the Risk ID
 - Column Eight - Risk ID's short description
 - Column Nine - Risk ID's detailed description
 - Column Ten - Risk Level
 - Column Eleven - Risk Status (0 = Enabled, 1 = Disabled)

NOTE: These files contain the default values recommended by Virsa Systems. You may want to edit the contents of each file before running the Conversion Wizard so the Rules generated from the table data in each file are customized for your location.

You can disable individual transactions in the function_tcode.txt file and Risks in the risks.txt file so they are not used to generate Rules.

To disable transactions change the '0' in the second column to a '1'.

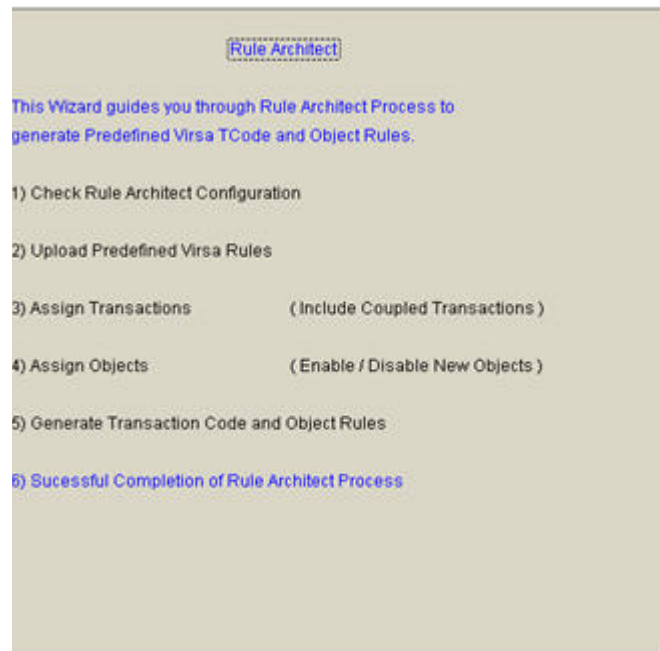
To disable Risks change the '0' in column eleven to a '1'.

In order for the Wizard to work these files must be copied to a directory on the server hosting Compliance Calibrator -

- Create a directory on the host server and note the full pathname. You'll need to specify the full pathname in Step Two.
- You must have read/write access to the directory you are creating on the server.
- The Wizard performs a case-sensitive search during the conversion process. The filenames should all be lowercase.

Running the Rule Architect Wizard

Figure 8–13: Rule Architect Wizard



Step One - Check Rule Architect Configuration

The first step the wizard performs is to check the status of the Rule Architect Activation Configuration Option. This option's value must be set to YES for the conversion process to begin.

Step Two - Upload Predefined Virsa Rules

This step asks you to create a directory and copy the pre-defined data files to it. These are the file used to create Functions and Risks in the Rule Architect. Please check the following -

- You must have read/write access to the directory you are creating on the server.
- The filenames the wizard looks for are case-sensitive. Use lower case for everything.
- You need to specify the full pathname of the directory you created. Please check the following -
 - For Windows OS Servers - Make sure all the slashes are backslashes (as shown in the figure below).
 - For UNIX Servers - Make sure all the slashes are forward slashes
 - Make sure you include the final slash

Figure 8–14: Rule Architect Wizard - Step Two, Upload Predefined Data



Step Three - Assigning transactions

CAUTION: If you are using SAP Compliance Calibrator by Virsa Systems version 4.6b, please skip to Step Four. SAP Compliance Calibrator by Virsa Systems version 4.6b does not support the Coupled Transaction feature.

This step displays a list of all coupled transactions. SU24 is used to identify all your coupled transactions. Click the checkbox for those coupled transactions you want to include when you generate new transaction code level and authorization object level Rules in Step 5.

Step Four - Assigning Objects

This step lists the Predefined Virsa Objects not included in your custom Rules table and the custom objects not included in the Predefined Virsa Objects table. Check each object you want to include when you generate new Authorization Object level Rules.

Figure 8–15: Rule Architect Wizard - Step Four, Specifying Objects for Rule Generation

Predefined Virsa Objects					
Customer New Objects					
Table	Function	TCode	Object	Field	From
<input type="checkbox"/>	AP01-APPayments	F-04-PostwithClearing	AccountingDocumentAuthorizationforAccount...	Accounttype(KOART)	K-Vendors
<input type="checkbox"/>	AP01-APPayments	F-07-PostOutgoingPayments	AccountingDocumentAuthorizationforAccount...	Accounttype(KOART)	K-Vendors
<input type="checkbox"/>	AP01-APPayments	F-18-PaymentwithPrintout	AccountingDocumentAuthorizationforAccount...	Accounttype(KOART)	K-Vendors
<input type="checkbox"/>	AP01-APPayments	F-31-PostOutgoingPayments	AccountingDocumentAuthorizationforAccount...	Accounttype(KOART)	K-Vendors

Step Five - Generate Transaction Code and Object Rules

We recommend you generate your new Rules in the background to make sure there is no server timeouts during generation.

Upload/Download Compliance Calibrator Tables

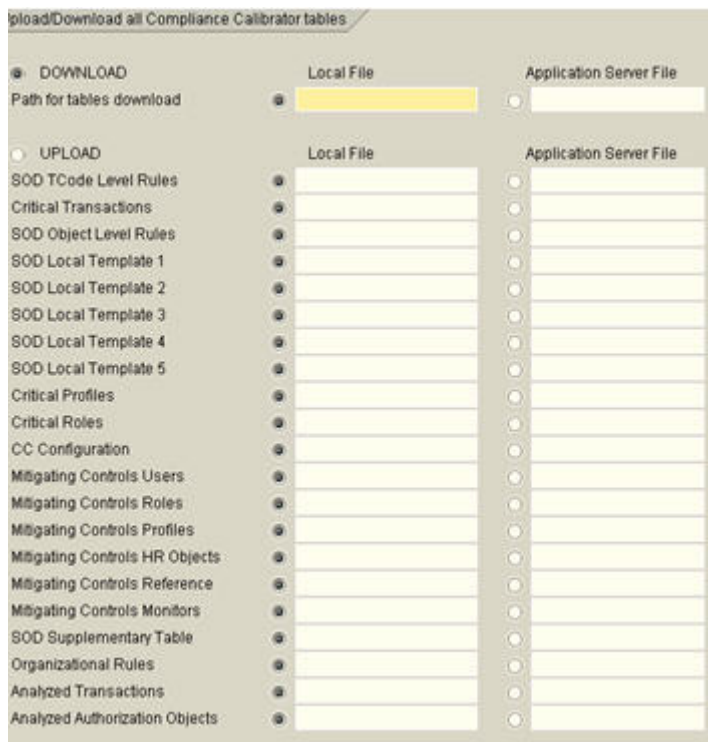
This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > Miscellaneous > Virsa Upgrade Tools

You can use this utility to upload data into any table or download the data from all tables.

CAUTION: There is no 'append' functionality with this utility. Tables uploaded to Compliance Calibrator will overwrite any entries currently in the tables.

Figure 8–16: Upload/Download Compliance Calibrator Table



Download Spool Request by Job Name

This report can be found in the Tool Box in the following location -

Virsa Utilities & Reports > Miscellaneous

If you have the Configuration Option Multiple Spool Options set to YES multiple jobs may be created when you generate Risk Analysis reports in the background. Use this utility to download all the spooled jobs.

Figure 8–17: Download Spool Requests by Job Name



NOTE: If there is more than one file to be downloaded, the report adds extensions to the file name entered above as 001, 002, 003 and so on depending on the number of downloaded files.

NOTE: Please refer to SAP Note #861556 for information regarding the installation procedures for SAP Compliance Calibrator by Virsa Systems.

Appendix A. Configuration Options

Introduction

Compliance Calibrator has various configuration options that allow Users to use Compliance Calibrator more effectively and efficiently. Default settings for various selections in the Compliance Calibrator control panel screen may be customized by setting these options.

NOTE: Compliance Calibrator performs validation on the configuration options so only accepted values may be saved.

Validation also prevents multiple iterations of a configuration options. The three exceptions to creating multiple iterations are -

- Risk ID (Risk Analysis Options)
- Cross-System ID (Risk Analysis Options)
- RFC Destination for Remote Simulation (Risk Analysis Options)

The various options are arranged under the following categories -

- Rule Architect Options
- Mitigation Controls Options
- Risk Analysis Options
- Report Options
- Program Options

Rule Architect Options

Rule Architect Activation

Setting this option to NO provides the ability to maintain the Conflicting Transactions and Authorization Objects Rules table directly. The tables can be accessed through the Rule Architect. If this option is set to NO the Update Rules button, appearing in the Function forms and Risk forms of the Rule Architect is grayed out and cannot be used to update the Rules tables. The default value is NO.

CAUTION: It is recommended that you set this option to YES and maintain your Rules using the Rule Architect features, rather than editing the Transaction Code Level and Authorization Object Level Rules tables directly.

Mitigation Controls Options

Date Range Limit for Mitigating Controls

When you assign a Mitigation Control to a Risk you must specify the validity period of the Control. If you leave the "To Date" blank the value in this option is used to calculate the end date of the validity period. The default value is 365 (days).

Enable Business Unit Authorization Check for Mitigation

Business Units available for assignment to a Mitigation Control are determined by your User ID and the Compliance Calibrator Role you are assigned. If this option is set to YES only authorized Business Units may be assigned to the Mitigation Control you are defining. The default value for this option is NO.

Enable User Group Authorization Check for Mitigation

The Compliance Calibrator Role assigned to your User ID determines which Users you can assign a Mitigation Control. The default value for this option is NO. Setting the value to YES limits the Users you can mitigate.

Enable Risk Level Authorization Check for Mitigation

The Compliance Calibrator Role assigned to your User ID determines which Risk Levels (Critical, High, Medium, Low, All) of a Risk you can assign a Mitigation Control. The default value for this option is NO. Setting the value to YES limits the Risks you can mitigate.

Enable Role Level Authorization Check for Mitigation

The Compliance Calibrator Role assigned to your User ID determines which Roles you can assign a Mitigation Control. The default value for this option is NO. Setting the value to YES limits the Roles you can mitigate.

Enable HR Object Level Authorization Check for Mitigation

The Compliance Calibrator Role assigned to your User ID determines which HR Objects you can assign a Mitigation Control. The default value for this option is NO. Setting the value to YES limits the HR Objects you can mitigate.

Risk Analysis Options

Default Type of Report

This option sets the default Report Type when running a Risk Analysis. The default value is ST. The accepted values are -

ST	SoD at Transaction Code Level
SA	SoD at Authorization Object Level
CT	Critical Transaction
CR	Critical Roles
MC	Mitigating Controls

Default Risk Level

This option sets the default Risk Level when running a Risk Analysis. The default value is ALL. The accepted values are -

CRIT	Critical
HIGH	High
MED	Medium
LOW	Low
ALL	

Default User Type

This option sets the default User Types included when running a Risk Analysis. The default is Dialog. The accepted values are -

DIA	Dialog
SYS	System
REF	Reference
COM	Communication
SER	Service
ALL	

Include Reference User in User Analysis

Any User referencing another User ID inherits the use of the referenced User's authorization objects. If this option is set to YES, the referenced User's authorization objects are included in the Risk Analysis. The default value for this option is NO.

NOTE: If you view the generated Risk Analysis report in detail view, the SoDs appear in a different color.

Ignore All Critical Roles/Profiles

This option specifies whether or not Roles and Profiles maintained in the Critical Roles table and the Critical Profiles table are ignored when running a Risk Analysis. The default value is NO. Setting the value to YES ignores all critical Roles and Profiles.

Set Locked Users

This option specifies whether or not Locked Users are excluded when running a Risk Analysis. The default value is YES.

Setting the value to YES places a checkmark next to Locked Users in the Exclusions section of the Risk Analysis form and excludes Locked Users when running a Risk Analysis.

Set Expired Users

This option specifies whether or not Expired Users are excluded when running a Risk Analysis. The default value is YES.

Setting the value to YES places a checkmark next to Expired Users in the Exclusions section of the Risk Analysis form and excludes Expired Users when running a Risk Analysis.

Set Mitigating Control

This option specifies whether or not Risks with Mitigating Controls are excluded when running a Risk Analysis. The default value is NO.

Setting the value to YES places a checkmark next to Mitigating Controls in the Exclusions section of the Risk Analysis form and excludes Risks with Mitigating Controls when running a Risk Analysis.

Cross-System ID

This option defines the names of the cross systems you can run a Risk Analysis. The names defined through this option appear in the pop-up menu in the Systems section of the Risk Analysis form. You can create multiple iterations of this option to include multiple names to choose from a list. Each iteration of the option defines a different cross-system ID

RFC Destination for Remote Simulation

This option specifies the different RFC destinations that may be used when running remote simulations.

NOTE: In order to avoid the need to log into a remote system when running the simulation the RFC definition should include a User ID and password.

Use SoD Supplementary Analysis

This option determines whether or not the SoD Supplementary table is used when running a Risk Analysis. The default value is NO. If you set the value to YES the SoD Supplementary table is used when running a Risk Analysis. See section 1.16, Building an SoD Supplementary Table for more information.

Use AND Option in Users & User Groups

This option determines if a Risk Analysis is run against both Users AND User Groups. If you set this option to YES both the Users and User Groups specified in the Analysis Type component of the Risk Analysis form are used when running a Risk Analysis.

The default value is NO. If you set the option to NO you can have values in the Users field and the User Groups field of the Analysis Type component, but the Risk Analysis only includes the Users OR User Groups, depending on which radio button is selected.

Risk ID

This option defines the list of Risk IDs appearing in the pop-up menu for the Report Type Risk ID filter. You can create multiple iterations of this option. Each iteration defines another Risk ID appearing in the pop-up menu.

You can use any character string as a value for this option e.g. F*,

Report Options

Display Long Risk Description

This option allows Users to configure the length appropriate for the display of the Risk Description. The length of the description field is 132 characters. Setting this parameter to NO allows only the first 60 characters to be displayed in the on-line reports. The default value is NO.

Show All in Report

Setting this option to YES specifies all Users included in your Risk Analysis should appear in the Risk Analysis report, regardless of whether the analysis generates any SoDs for the User. If a User does not have any SoDs the report displays "No Conflicts". The default value for this option is NO. If the option is set to NO, Users with no conflicts are not included in the Risk Analysis report.

Show Composite Role in User Analysis

Setting the value of this option to YES adds a column to Risk Analysis reports. The additional column is used to identify the composite role in a Role-based Risk Analysis. The default value is NO.

Default Report Format

Setting this option determines the default report format when running a Risk Analysis. The values for this option are -

ESUM	Executive Summary
SUM	Summary
DET	Detail

Set Default Business View

Setting this option to YES places a checkmark next to Business View in the Report Format component of the Risk Analysis form. The default value is YES.

Compliance Calibrator Tables Display Format (Tab/ALV)

The Compliance Calibrator tables display format parameter, can be set to either TAB or ALV display. Default is TAB.

Customer Specific Header Text

The text entered in the Customer specific Header Text will appear on the top of every page of all Compliance Calibrator reports.

Include Role/Profile Mitigating Controls in User Analysis

Setting this option to YES includes any Role- or Profile-based Mitigation Control IDs in User-based Risk Analysis reports. The default value is NO.

Security & Controls Policies & Procedures

The name of the document containing the Company's Security & Controls Policies and Procedures information can be entered here.

Program Options

Memory Variable for Batch Size

This option affects how a local User-based Risk Analysis is run in the background. The option determines the number of authorizations included when running the background analysis. The default value is 5000 (if you leave the value blank it assumes 5000). If you set the value to 0 each user is run one at a time.

Batch Size for Users

This option determines how many Users are processed at one time during a background Risk Analysis. The default value is 100 (if you leave the value blank it assumes 100).

Batch Size for Roles

This option determines how many Roles are processed at one time during a background Risk Analysis. The default value is 100 (if you leave the value blank it assumes 100).

Multiple Spool Options

This option determines if multiple spools are created when running a Risk Analysis in the background. This option is used in combination with Batch Size for Users and Batch Size for Roles. The default value is NO. If you set the value to YES the number of Users or Roles spooled is determined by the value the Batch Size for Users and Batch Size for Roles options. When the number of Users or Roles specified is reached a new spool job is created.

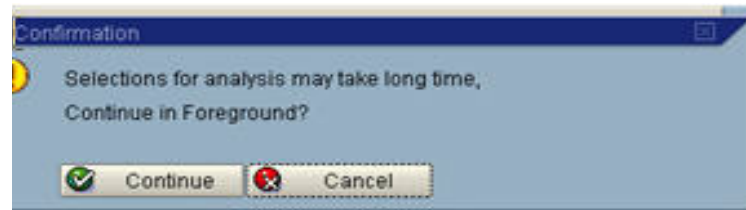
It is advantageous to use this option when running a Risk Analysis on a large number of Users or Roles to avoid spool errors and memory issues.

NOTE: You can use transaction SP01 to view each spooled report separately, or you can use the Download Spools utility in the Compliance Calibrator Tool Box to combine and view all the spools as one report.

Threshold Value for Users Analysis

This option determines the number of Users included in a foreground Risk Analysis without displaying a confirmation warning. The default value is 10.

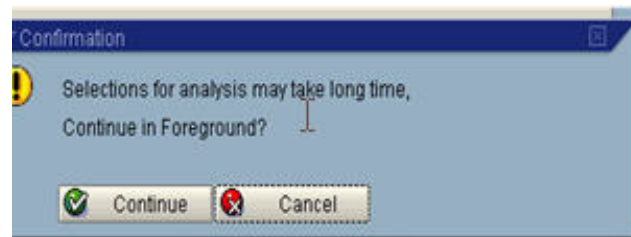
Figure A-1: Confirm Foreground Processing Above User-Based Threshold Levels



Threshold Value for Role/Profile Analysis

This option determines the number of Roles or Profiles included in a foreground Risk Analysis without displaying a confirmation warning. The default value is 10.

Figure A-2: Confirm Foreground Processing Above Role/Profile-Based Threshold Levels



Cross-System SoD Analysis

This option works in combination with the Cross System ID option. Setting this option to YES allows cross-system analysis to be performed. The default value is NO.

System Administrator Lock

This option locks all Compliance Calibrator tables except the Configuration Options table. If the value is set to YES no tables may be updated or maintained. The default value is NO.

PFCG Plugin

This option determines if Virsa's Risk Terminator should be initiated. The default value is NO. If you set the value to YES Risk Terminator should be installed on the same system as Compliance Calibrator.

NOTE: Please refer to SAP Note #861556 for information regarding the installation procedures for SAP Compliance Calibrator by Virsa Systems.

Enable Delta Analysis

Delta analysis improves Compliance Calibrator's performance by storing Risk Analysis data in tables for Users, Roles, Profiles, and HR Objects. The default value is NO. If you set the value to YES the data is stored and used.

When this option is turned on Compliance Calibrator checks to see if a User, Role, Profile, or HR Object has been changed. If it hasn't and an analysis has already been run against it the stored data is used in the generated report.

This option affects only background analyses.

CAUTION: If you generate any new Rules after running Risk Analyses with this option set to YES you must force a full scan in order to re-analyze all Users, Roles, and Profiles stored in the tables maintained by the option. To do this, check Force Full Scan when you run a background analysis.

Custom Utilities

This parameter determines if the Custom Utilities appears on the menu bar. The default value is NO. If the option is set to YES the Custom Utilities menu is displayed on the menu bar.

Log file location

Duplicate records may be logged when uploading records to Compliance Calibrator. To log duplicates, define a directory in the configuration parameter (Log File Location). A file will be created and saved to that directory name (program name + date + time). Duplicate records will be saved in this file. Default value is root path (C:\).

Rule Batch size for New Compliance Calibrator BAPI

The default value for this option is 1000.

This option is only used when Compliance Calibrator is accessed through Virsa's Access Enforcer. The number of Rules used for analysis is batched according to the option value to address memory issues.

NOTE: Please refer to SAP Note #861556 for information regarding the installation procedures for SAP Compliance Calibrator by Virsa Systems.

Appendix B. Not Logic

Introduction

The following examples explain the use of the logical operator NOT in SoD Rule tables.

SOD rule with one NOT

A User SOD conflict will appear if the User's authorizations satisfy all the lines except the one with NOT. The User must not have object V_KNA1_VKO with field ACTVT and value 06 to satisfy this conflict.

Group N.	Object	Field	from	to	AND/OR	Risk Description	Risk Level	Status
TEST_NOT	F_BKPF_BUK	ACTVT	01	02		CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
TEST_NOT	F_BKPF_BUK	BUKRS	MX20			CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
TEST_NOT	F_BKPF_KOA	ACTVT	01	02		CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
TEST_NOT	F_BKPF_KOA	KOART	K			CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
TEST_NOT	S_TCODE	TCO	FBZ1			CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
TEST_NOT	S_TCODE	TCO	XD06			CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
TEST_NOT	V_KNA1_VKO	ACTVT	01	02		CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
TEST_NOT	V_KNA1_VKO	ACTVT	06		NOT	CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
TEST_NOT	V_KNA1_VKO	VKORG	MX20			CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable

SOD rule with two or more NOT for different Object/Field combinations

A User SOD conflict will appear if the User's authorizations satisfy all the lines except the two lines with NOT. The User must not have object F_BKPF_BUK with field ACTVT and value 06 and object V_KNA1_VKO with field ACTVT and value 06 to satisfy this conflict.

up N.	Object	Field	from	to	AND/OR/NOT	Risk Description	Risk Level	Status
T_NOT	F_BKPF_BUK	ACTVT	01	02		CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
T_NOT	F_BKPF_BUK	ACTVT	06		NOT	CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
T_NOT	F_BKPF_BUK	BUKRS	MX20			CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
T_NOT	F_BKPF_KOA	ACTVT	01	02		CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
T_NOT	F_BKPF_KOA	KOART	K			CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
T_NOT	S_TCODE	TCO	FBZ1			CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
T_NOT	S_TCODE	TCO	XD06			CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
T_NOT	V_KNA1_VKO	ACTVT	01	02		CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
T_NOT	V_KNA1_VKO	ACTVT	06		NOT	CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
T_NOT	V_KNA1_VKO	VKORG	MX20			CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable

SOD rule with two or more NOT for same Object/Field combinations

A User SOD conflict will appear if the User's authorizations satisfies all the lines except the two lines with NOT. So it must not have object V_KNA1_VKO with field ACTVT and value 05 and object V_KNA1_VKO with field ACTVT and value 06 to satisfy this conflict.

Sup N	Object	Field	from	to	AND/OR Risk Description	Risk Level	Status
ST_NOT F	BKPF_BUK	ACTVT	01	02	CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
ST_NOT F	BKPF_BUK	BUKRS	M:20		CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
ST_NOT F	BKPF_KDA	ACTVT	01	02	CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
ST_NOT F	BKPF_KDA	KDART	K		CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
ST_NOT S	TCODE	TCO	FBZ1		CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
ST_NOT S	TCODE	TCO	XD06		CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
ST_NOT V	KNAT_VKO	ACTVT	01	02	CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
ST_NOT V	KNAT_VKO	ACTVT	05		NOT CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
ST_NOT V	KNAT_VKO	ACTVT	06		NOT CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable
ST_NOT V	KNAT_VKO	VKORG	M:20		CUSTOMER MASTER and INCOMING PAYMENTS	High	Enable

- Click Execute to install Compliance Calibrator.
This will take some time to install.

Appendix C. Defining RFC Destinations

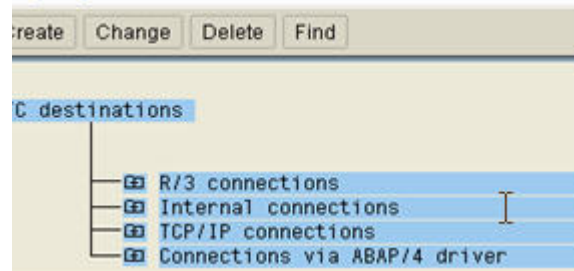
Introduction

In order to run a cross-system Risk Analysis or Simulation you need to define an RFC for each remote system. You can use SM59 to define your RFCs.

Defining an RFC

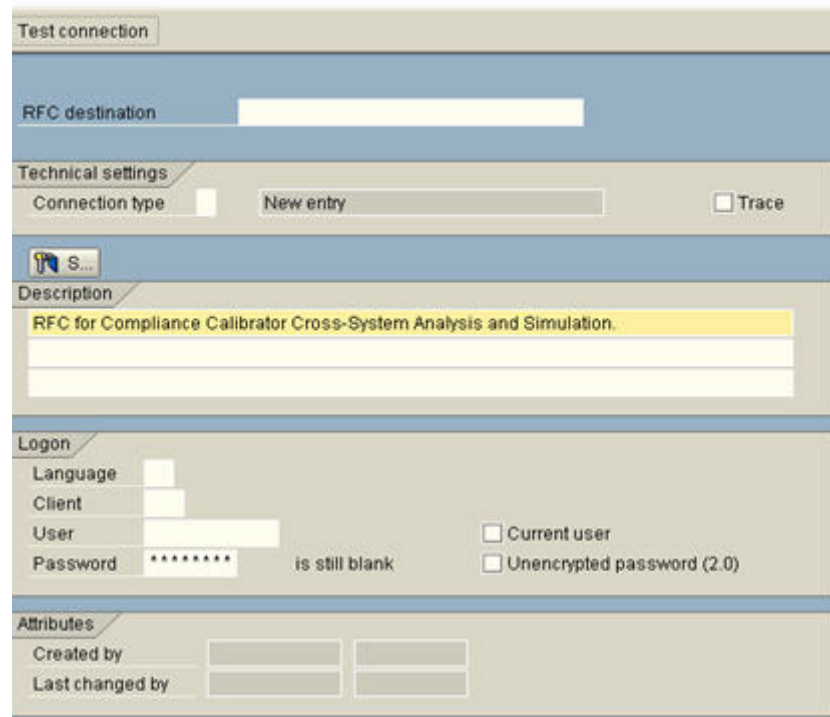
1. Run SM59

Display and maintain RFC destinations



2. Click on R/3 connections and then click Create.
3. Fill in the following fields in the form below -
 - RFC destination
 - Description
 - Language
 - Client
 - User & Password

RFC Destination



NOTE: The User and Password you hard code into your RFC must exist on both your Local system (the system Compliance Calibrator is installed on) and the Remote system the RFC is calling. The User ID you use should be of type Service so that the password never expires.

4. Click Execute to install Compliance Calibrator.
This will take some time to install.

Appendix D. Using a Non-sequential Range of Values

Introduction

Compliance Calibrator supports lists of non-sequential values when running a Risk Analysis. When you want to run a Risk Analysis on a range of Users not in alphabetic sequence, you can use the Multiple Selection button and specify any set of values.

Multiple values may be entered manually or uploaded from a tab-delimited file. The procedure below assumes your values are stored in a tab-delimited file.

Importing a Text File

1. Click the Multiple Selection icon to display the entry form.
2. The icon appears to the right of any Risk Analysis field that supports the feature.
3. Click the Import from Text File icon.
Enter the name of the tab-delimited file containing your field values in the File name field.
4. Click the Upload from Clipboard icon to copy the field values.
5. Use Control-V to paste your values into the field on the Single vals tab.
6. Click Execute to return to the Risk Analysis control panel screen.

NOTE: Please refer to SAP Note #861556 for information regarding the installation procedures for SAP Compliance Calibrator by Virsa Systems.

Appendix E. Long Descriptions in Transport Requests

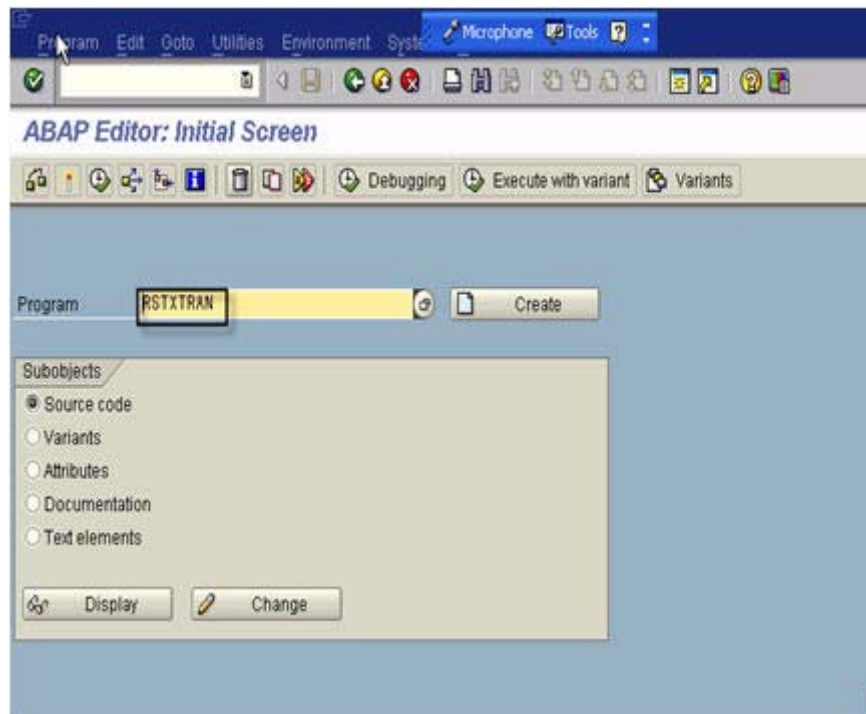
Introduction

When you use the Mass Transport utility in Rule Architect and Mitigation Controls you must use SE38 to add the values stored in the following description fields. Use the procedure below for each field name.

- /VIRSA/MIT - Mitigation Description
- /VIRSA/RIS - Summary Risk Description
- /VIRSA/RSO - Risk Control Objective
- /VIRSA/ALT - Detailed Risk Description

Adding Long Descriptions to the Transport

1. Call Transaction SE38, run program 'RSTXTRAN' and then click Execute.



- Enter the field name for one of the description fields from above and click Execute.

The screenshot shows the SAP Script Editor window with the title bar 'Program Edit Goto System Help'. The main window title is 'Transfer of SAPscript Texts to a Correction'. Below the title bar is a toolbar with various icons. The main area contains a form with the following fields:

Name of correction	
Text key - object	/VIRSA/MIT
Text key - name	
Text key - ID	LTXT
Text key - language	EN

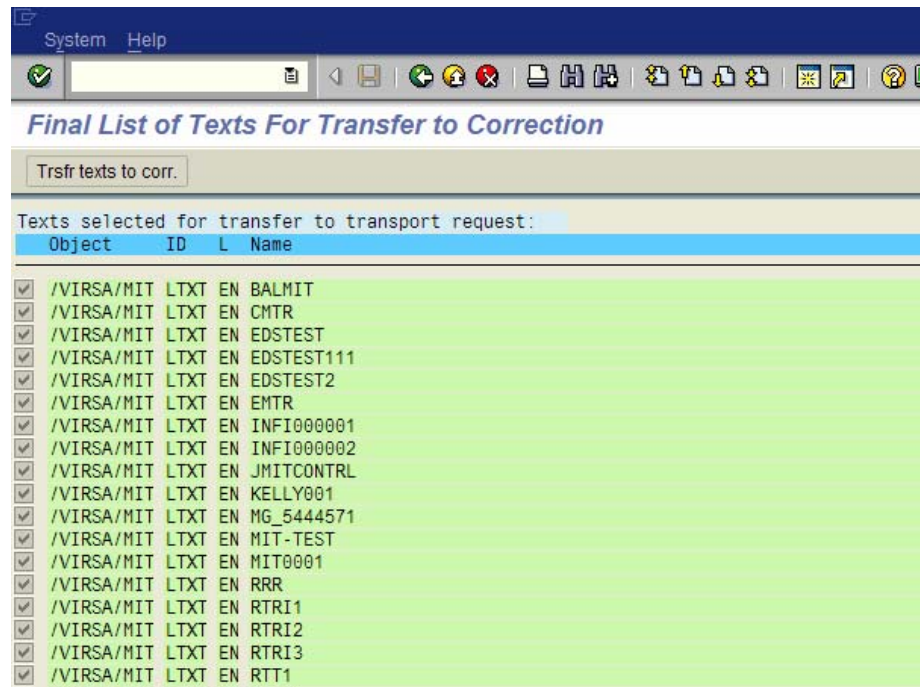
- The following Provisional list is displayed.
If all the objects are not selected click Select All, then click Execute.
The Final list is then displayed.

The screenshot shows the SAP Script Editor window with the title bar 'System Help'. The main window title is 'Provisional List of Texts to be Transferred'. Below the title bar is a toolbar with various icons. The main area contains a form with the following fields:

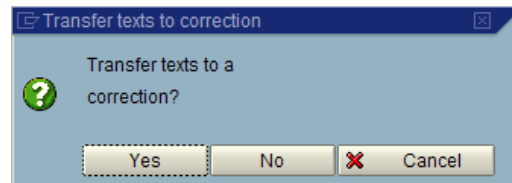
Select All Deselect All

Please select the texts to be transported:

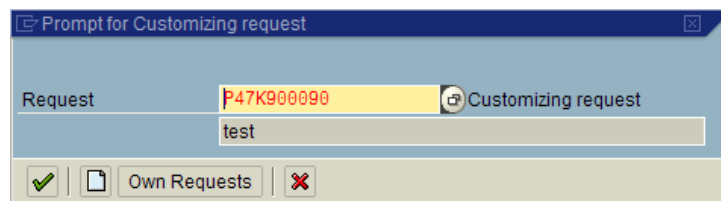
Object	ID	L	Name
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN BALMIT
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN CMTR
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN EDSTEST
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN EDSTEST111
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN EDSTEST2
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN EMTR
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN INFI000001
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN INFI000002
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN JMITCONTRL
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN KELLY001
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN MG_5444571
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN MIT-TEST
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN MIT0001
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RRR
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RTRI1
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RTRI2
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RTRI3
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RTT1
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RTT10
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RTT2
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RTT3
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RTT4
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RTT5
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RTT6
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RTT7
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN RTTT
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN TECA
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN TEST
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN TESTMIT
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN TEST_PM1
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN TEST_PM2
<input checked="" type="checkbox"/>	/VIRSA/MIT	LTXT	EN Z339040



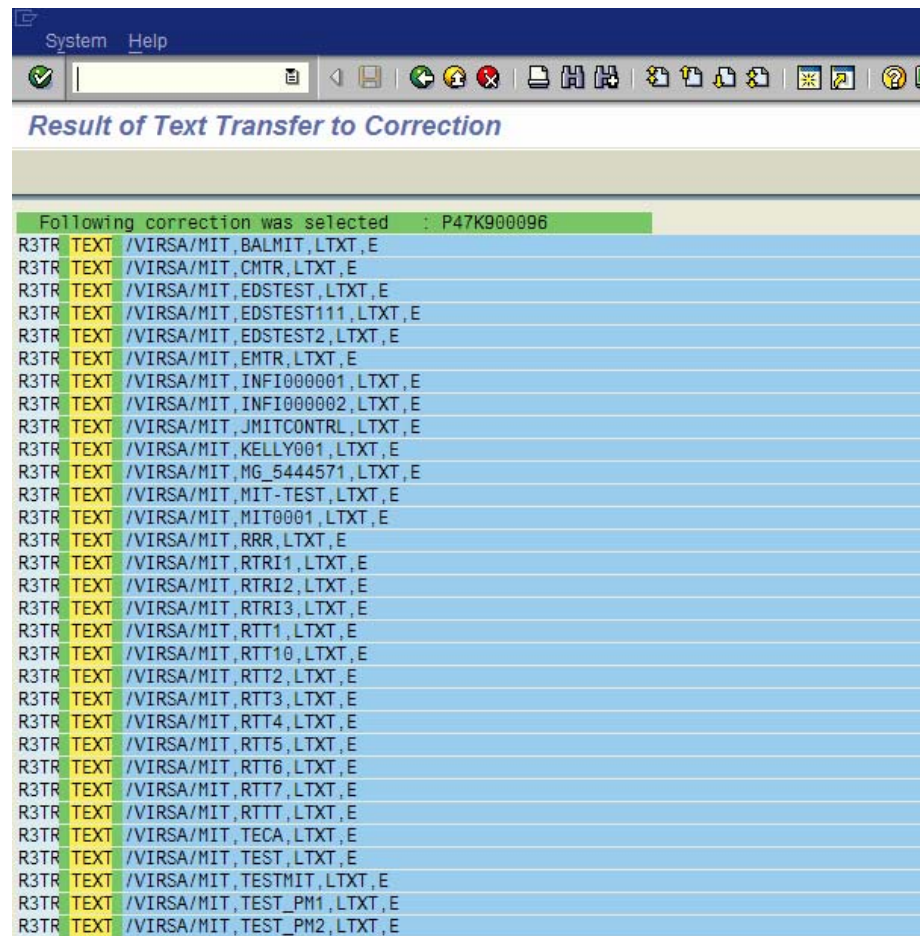
- Click Trsfr texts to corr. to add the entries to your transport request. Click Yes when the following prompt is displayed.



- Enter a transport request number you used when creating the mass transport and then click Execute.



6. The following screen displays all the entries transferred to the transport request.



7. Click Execute to install Compliance Calibrator.
This will take some time to install.

Appendix F. Post Installation Customization

Delivery Customizing

On installation, data is imported into 000 clients. Once imported, data may be copied into other clients if required. For more information, see SAP Notes 337623 and 861556.

Installing Virsa Objects

The installation package contains BC sets, you will need to activate these. In order to activate them you will need the names of the BC Sets and transaction SCPR20. The activation must take place in the client to which you need the data transferred. Please activate the BC Sets as Background jobs (using the Background Job option). You will need to activate the BC Sets in the following sequence:

/VIRSA/ZTAB	Table Contents
/VIRSA/ZAUTH	Authorization Object Entries

CAUTION: The object /VIRSA/ZAUTH (Authorization Object Entries) contains non-namespace objects. Please make sure that these objects are not already in use in your system.

/VIRSA/ZVRATCNFG	Configuration Table Entries BC Set
/VIRSA/ZRULES	Rule Set 1
/VIRSA/ZSODTC	SOD Tcode Rules BC Set
/VIRSA/CRAUTH1	Authorization Object Rules 1
/VIRSA/CRAUTH2	Authorization Object Rules 2
/VIRSA/CRAUTH3	Authorization Object Rules 3
/VIRSA/CRAUTH4	Authorization Object Rules 4
/VIRSA/CRAUTH5	Authorization Object Rules 5
/VIRSA/CRAUTH6	Authorization Object Rules
/VIRSA/CRAUTH7	Authorization Object Rules 7

When activating Virsa BC-Sets make sure to use the Overwrite Activation Option > Overwrite Data > Overwrite All Data.

NOTE: Please execute report RSCLCCOP using transaction SA38 to copy Virsa related data from one client to another client for transport SAPK-400COINVIRSA.