

## User Guide



# Risk Terminator™ Version 4.0

with Compliance Calibrator for SAP

Note: The actual application will display V1.2  
This was the version number before SAP rebranding.

## **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**

# CONTENTS

## Preface

About this Guide .....	6
Conventions .....	6
Alert Statements .....	6
Product Documentation .....	7
Documentation Formats .....	7
Installation Guide, Configuration Guide, User Guide, and Release Notes .....	7
Online Help .....	7
Contacting Virsa Systems .....	8

## 1 Risk Terminator—Segregation of Duties

Introduction .....	10
Segregation of Duties (SoD) Concept .....	10

## 2 Overview

Introduction .....	12
Configuring Risk Terminator .....	12
Field Definitions .....	13

## 3 Using Risk Terminator

Introduction .....	16
When Transactions Are Added to a Role and the Role is Generated Using PFCG .....	16
When User(s) Are Assigned to a Role Using PFCG .....	20
When Role/Profile is Assigned to a User Using SU01 .....	21
When Role/Profile is Assigned to User(S) Using SU10 .....	22

## 4 Risk Terminator Log Reports

Introduction .....	24
--------------------	----

**A     Installing Risk Terminator**

    Introduction .....26

**B     Deleting a Role Lock**

    Introduction .....28

# PREFACE

---

## TOPICS COVERED IN THIS PREFACE

[About this Guide](#)

[Conventions](#)

[Alert Statements](#)

[Product Documentation](#)

[Documentation Formats](#)

[Installation Guide, Configuration Guide, User Guide, and Release Notes](#)

[Online Help](#)

[Contacting Virsa Systems](#)

## About this Guide

### Conventions

The following conventions are observed throughout this document:

- **Bold** sans-serif text is used to designate file and folder names, dialog titles, names of buttons, icons, and menus, and terms that are objects of a user selection.
- **Bold** text is used to indicate defined terms and word emphasis.
- *Italic* text is used to indicate user-specified text, document titles, and word emphasis.
- Monospace text (`Courier`) is used to show literal text as you would enter it, or as it would appear onscreen.

### Alert Statements

The alert statements—Note, Important, and Warning—are formatted in the following styles:



---

**Note** Information that is related to the main text flow, or a point or tip provided in addition to the previous statement or instruction.

---



---

**Important** Advises of important information, such machine or data error that could occur should the user fail to take or avoid a specified action.

---



---

**Warning** Requires immediate action by the user to prevent actual loss of data or where an action is irreversible, or when physical damage to the machine or devices is possible.

---

## **Product Documentation**

### **Documentation Formats**

Documentation is provided in the following electronic formats:

- Adobe® Acrobat® PDF files
- Online help

You must have Adobe® Reader® installed to read the PDF files. Adobe Reader installation programs for common operating systems are available for free download from the Adobe Web site at [www.adobe.com](http://www.adobe.com).

### **Installation Guide, Configuration Guide, User Guide, and Release Notes**

You can download the Installation Guide, Configuration Guide, User Guide, and Release Notes in PDF format.

### **Online Help**

You can access online help by clicking the **Help** link from within the application.

---

## Contacting Virsa Systems

For information on contacting Virsa Systems, refer to the table below or the Virsa Web site [www.virsa.com](http://www.virsa.com).

If you have any questions about the Risk Terminator application, framework and its components, or would like to report a problem, please contact Virsa Global Support Services.

Phone/Fax Numbers		E-mail Address	Postal Mail Address
Within U.S.	1-888-847-7217 (1-888-VIRSA-17)	support@virsa.com	47257 Fremont Boulevard Fremont, CA 94538 USA
Outside U.S.	1-877-847-7268 (1-877-VIRSA-68)		
Direct Line	510-580-1079		
Fax	510-580-1414		



# RISK TERMINATOR— SEGREGATION OF DUTIES

---

## TOPICS COVERED IN THIS CHAPTER

Introduction

Segregation of Duties (SoD) Concept

## Introduction

Risk Terminator is an Advanced Business Application Programming (ABAP) based solution that works with SAP's Role Generator and User Assignment. Risk Terminator employs best practices to ensure that role generator and user assignment does not introduce risk through Segregation of Duties (SoD).

It helps Role Owners and Security Administrators create and maintain role definitions and identify potential Audit and SoD issues.

## 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 ensuring 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 SoDs - especially when dealing with cash, negotiable checks and inventories.

There are business processes where SoDs are extremely important. For example, in cash handling. Cash can be 'liquified' without leaving an auditable trail. Any department that accepts cash funds, has access to accounting records, or has control over any type of liquid asset should be concerned with SoDs. Some examples of incompatible duties are:

- Authorizing a transaction and receiving and maintaining custody of the asset that resulted from the transaction.
- Receiving payments 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. It is not always possible to have enough personnel to properly segregate duties. In those cases, management needs to take a more active role to achieve separation of duties and check the work done by others or using other Mitigating Controls.

# 2

## OVERVIEW

---

### TOPICS COVERED IN THIS CHAPTER

[Introduction](#)

[Configuring Risk Terminator](#)

---

## Introduction

This manual describes the Risk Terminator version 4.0 features and functionality running on SAP 4.6c and higher.

Risk Terminator, running PFCG, provides real-time reporting during role management and user assignment. When you create or modify a role and introduce a risk, Risk Terminator's reporting screens display the SoD.

Risk Terminator uses Compliance Calibrator's Transaction Code Rules and Authorization Object Rules Tables to determine if a SoD is being introduced to roles or users. Risk Terminator also uses Compliance Calibrator's Critical Transactions Table to check for any critical transactions being added to a role or assigned to a user.

## Configuring Risk Terminator

Risk Terminator is activated through the Compliance Calibrator. You can setup the configuration options in Compliance Calibrator for any of the following:

- **PFCG Plug-in** Generates a role. This option must be set to **Yes** to start Risk Terminator.
- **PFCG User Assignment Plug-in** Assigns users to a role. This option must be set to **Yes** for assigning users to a role.
- **SU01 Role Assignment Plug-in** Assigns a role to a user. This option must be set to **Yes** for assigning a role to a user.
- **SU10 Multiple User Role Assignment Plug-in** Assigns multiple roles to a user. This option must be set to **Yes** for assigning multiple roles to a user.



---

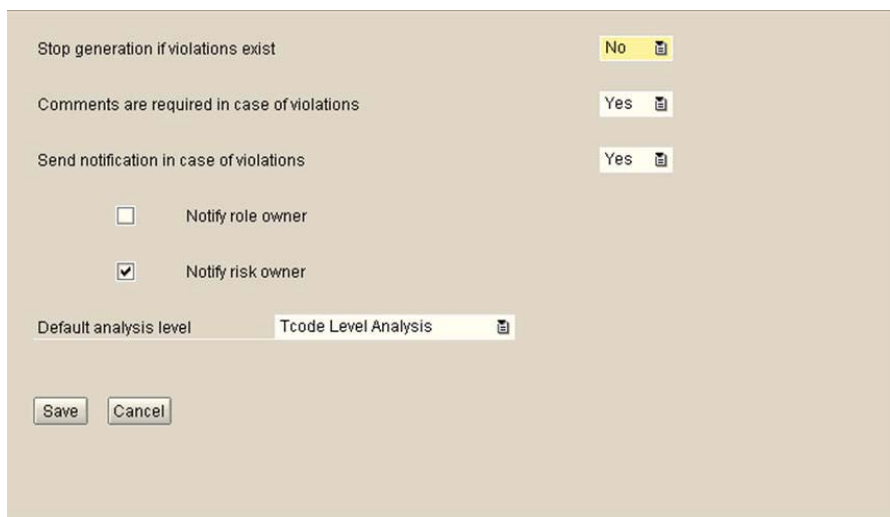
**Note** The default value for all above configuration options is **No**.

---

Refer to the Compliance Calibrator User Manual for more information on Compliance Calibrator configuration options.

In addition to setting the Compliance Calibrator configuration option, Risk Terminator has its own configuration screen.

To view the configuration option screen displayed below, enter the following transaction code into the command field `/n/VIRSA/ZRTCNFG` and click **Enter**.



The image shows a configuration screen for Risk Terminator. It has a light beige background. At the top, there are three rows of configuration options, each with a label on the left and a dropdown menu on the right. The first row is 'Stop generation if violations exist' with a dropdown set to 'No'. The second row is 'Comments are required in case of violations' with a dropdown set to 'Yes'. The third row is 'Send notification in case of violations' with a dropdown set to 'Yes'. Below these, there are two checkboxes: 'Notify role owner' (unchecked) and 'Notify risk owner' (checked). At the bottom, there is a 'Default analysis level' dropdown set to 'Tcode Level Analysis'. At the very bottom, there are 'Save' and 'Cancel' buttons.

**Figure 1** Risk Terminator Configuration Screen

### Field Definitions

- **Stop generation if violations exist** This field can be set to **YES** or **NO**. If it is set to **NO**, Role generation/User assignment using PFCG and User assignment using SU01 or SU10 is not affected.
- **Comments are required in case of violations** This field can be set to **YES** or **NO**. If it is set to **YES**, you are prompted to enter comments before continuing with Role generation/User assignment in PFCG or User assignment using SU01 or SU10. The information from the comments field can be viewed using the Risk Terminator Log Report.
- **Send notification in case of violations** This field can be set to **YES** or **NO**. If it is set to **YES** and you also check the Risk Owner checkbox an email is sent to the Risk Owner.

Risk Owners are defined through the **Compliance Calibrator Alerts Module Email Configuration** screen. If a Risk ID is associated with an email address specified in the Email Configuration screen, an email is sent to that email address. If no email address is associated with a Risk ID identified through Risk Terminator, no notification is sent to the Role Owner. Refer to your *Compliance Calibrator User Manual* for more information on using the email configuration screen.



**Note** The Notify role owner functionality of the Send Notification in case of violations option will be available in a future release.

- **Default Analysis Level** You can choose either TCode-level or Object-level analysis as the default. When Risk Terminator performs the Risk Analysis (when you click the Change authorization data button on the PFCG Authorizations tab), this field specifies the type of analysis performed.



---

**Note** The Default Analysis Level setting determines what level of SoD is reported by Risk Terminator. If the Default Analysis Level is set to Object Level Analysis, Risk Terminator will report Object-Level SoDs. On the report screen there is an option to perform TCode-level analysis and toggle between each report.

---

# 3

## USING RISK TERMINATOR

---

### TOPICS COVERED IN THIS CHAPTER

#### Introduction

- When Transactions Are Added to a Role and the Role is Generated Using PFCG
- When User(s) Are Assigned to a Role Using PFCG
- When Role/Profile is Assigned to a User Using SU01
- When Role/Profile is Assigned to User(S) Using SU10

# Introduction

Risk Terminator is activated in the following four cases:

- 1 When Transactions Are Added to a Role and the Role is Generated Using PFCG
- 2 When User(s) Are Assigned to a Role Using PFCG
- 3 When Role/Profile is Assigned to a User Using SU01
- 4 When Role/Profile is Assigned to User(S) Using SU10

A Risk Terminator report screen is displayed when you add any transactions using the **Menu** tab in PFCG and click the **Change Authorization Data** button or when you add transactions through the **PFCG Authorizations** screen and click the **Generate** button.

## When Transactions Are Added to a Role and the Role is Generated Using PFCG

When Risk Terminator is enabled, through the Compliance Calibrator’s PFCG Plug-in configuration option, the following steps are added to the PFCG Role generation process:

- 1 Add transactions through the **PFCG** menu tab.
- 2 Click **Change Authorization Data** on the **Authorizations** tab.

The **Risk Terminator** report screen appears.



Figure 2 Risk Terminator Transaction Code Level Risk Analysis Report



- 3 Click **Continue Profile Generation** to continue Role generation.



**Figure 3** Risk Terminator Warning

The following options are displayed:

- **Continue** If you click **Continue**, the **PFCG Authorizations** screen is displayed and any changes you have made through the **Menu** tab are included when you generate the Role.
- **Discard Changes** If you click **Discard Changes**, PFCG is exited and any modifications you have made to your Role are discarded. You must start the process over.
- **Mitigation** If you click **Mitigation**, the Compliance Calibrator's **Mitigation Controls** module is displayed. Refer to the *Compliance Calibrator User Manual* for more information about using the **Mitigation Controls** module.

From the **Mitigation Controls** module, you can search for an existing mitigation control for the Risk ID displayed on the **Risk Terminator** report screen, or you can create a new mitigation control, and then mitigate the risk by assigning controls to the Role. Click **Back** to return to the **Risk Terminator** screen.

Once you have mitigated any risks, click **Continue Profile Generation** to go to the **Authorizations** screen.

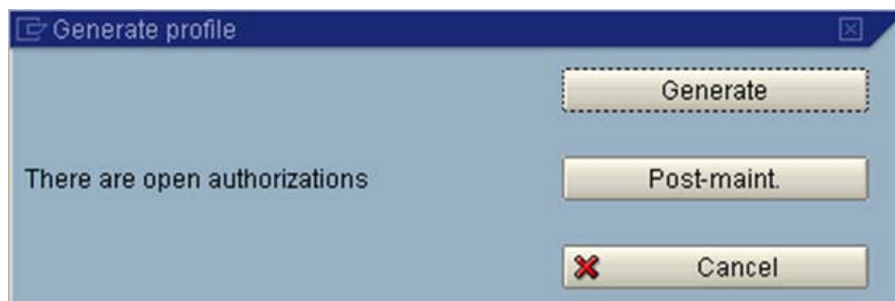


---

**Note** Risk mitigation does not affect Risk Analysis reports. If you make additional modifications to a Role, any SoDs previously mitigated are included in the Risk Analysis report generated by Risk Terminator. For more reporting options, see the *Compliance Calibrator User Manual*.

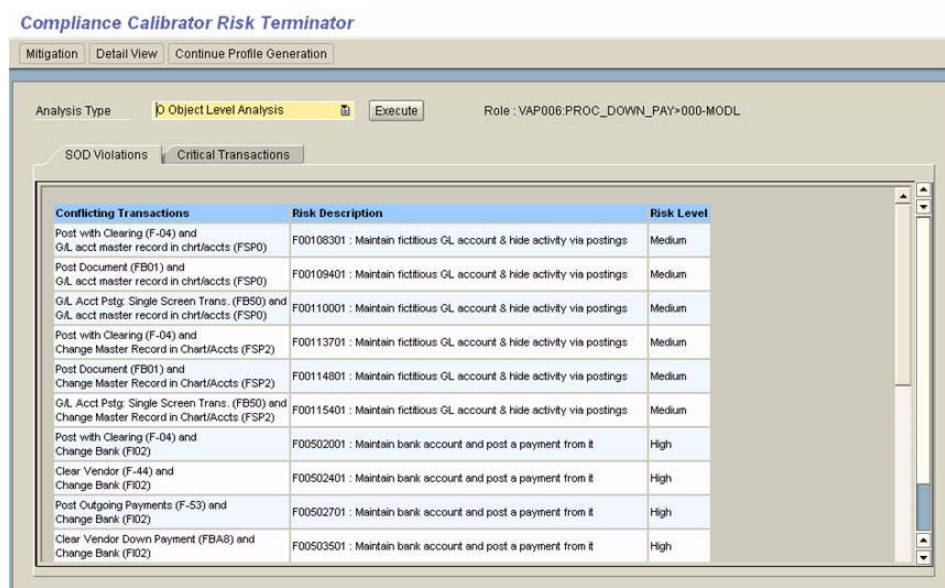
---

- 4 In the **Authorizations** screen, click **Generate**. The following window is displayed.



**Figure 4** Generate profile dialog

- 5 Click **Generate** and the following **Risk Terminator** screen is displayed. You can mitigate any reported SoDs.



**Figure 5** Risk Terminator Transaction Code Level Risk Analysis Report

- 6 Click **Continue Profile Generation** to display the following **Authorizations** screen.



**Figure 6** Risk Terminator Warning

- 7 Click **Discard Changes** to discard any modifications you have made to the Role and display the initial PFCG screen.
- 8 Click **Continue Simulation** to close the prompt and leave you in the **Authorizations** screen to continue making modifications. When you click **Generate** again, the **Risk Analysis** report screen is displayed to continue the process.
- 9 Clicking **Generate** to display the prompt displayed in [Figure 7 on page 19](#):



**Note** The following prompt is displayed if the role is generated with violations configuration option set to **YES**.

Risk Terminator Comment

Please specify the reason for generating role that is causing SOD Violations

Continue Back

**Figure 7** Logging a Reason for Causing an SoD Violation

- 10 Enter a justification for creating the SoD and click **Continue**. You can review the log of reasons by running the Risk Terminator report.

When User(s) Are Assigned to a Role Using PFCG

When you assign users using the **User** tab in PFCG and click **Save**, Risk Terminator checks for violations and if any are found the report screen is displayed as shown next.

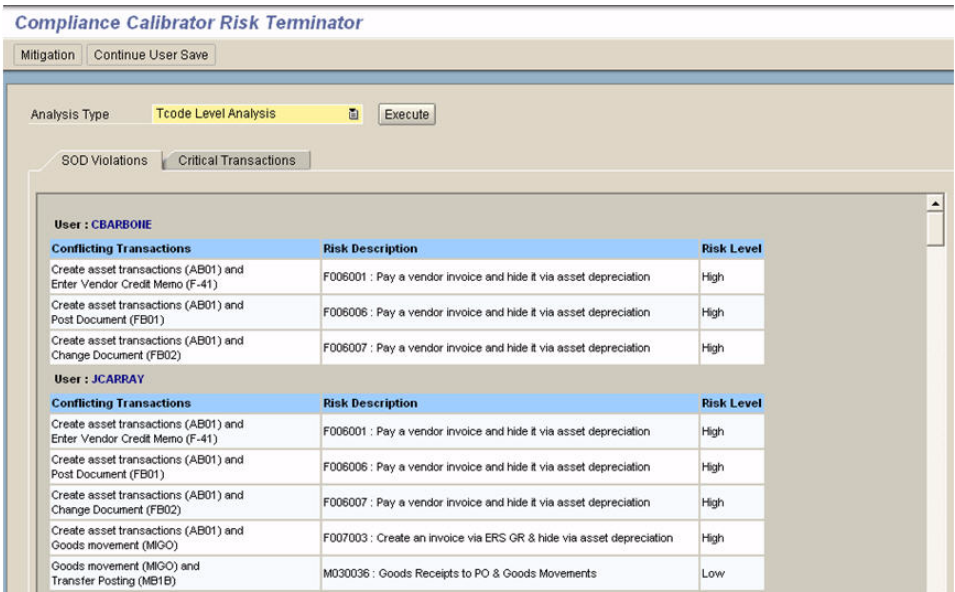


Figure 8 Risk Terminator Transaction Code Level Risk Analysis Report

If you click **Continue User** the following prompt is displayed.

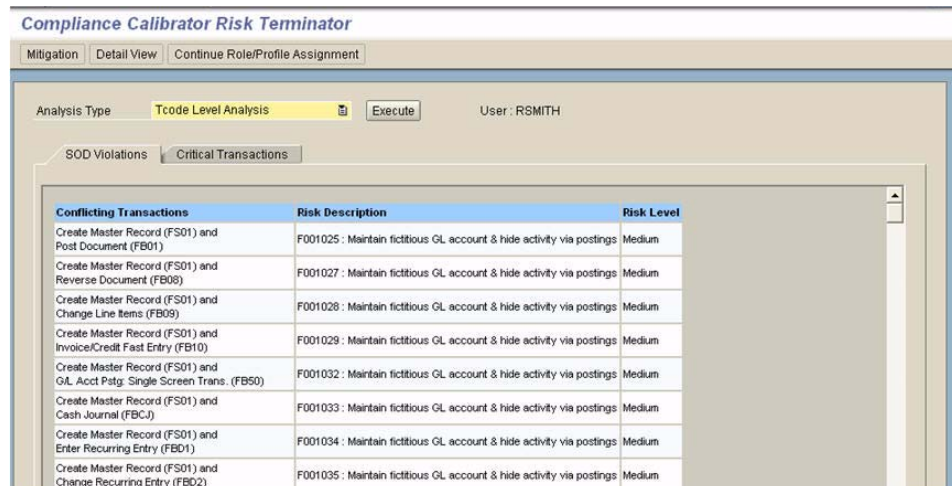


Figure 9 Risk Terminator Warning

- 1 Click **Discard Changes** to discard any user assignment you have made to the Role.
- 2 Click **Continue** to display the prompt as shown in [Figure 7](#).

## When Role/Profile is Assigned to a User Using SU01

When you assign a Role/Profile to a user using the **SU01** transaction and click **Save**, Risk Terminator checks for violations and if any are found the report screen is displayed as shown next.



Conflicting Transactions	Risk Description	Risk Level
Create Master Record (FS01) and Post Document (FB01)	F001025 : Maintain fictitious GL account & hide activity via postings	Medium
Create Master Record (FS01) and Reverse Document (FB08)	F001027 : Maintain fictitious GL account & hide activity via postings	Medium
Create Master Record (FS01) and Change Line Items (FB09)	F001028 : Maintain fictitious GL account & hide activity via postings	Medium
Create Master Record (FS01) and Invoice/Credit Fast Entry (FB10)	F001029 : Maintain fictitious GL account & hide activity via postings	Medium
Create Master Record (FS01) and GL Acct Patg: Single Screen Trans. (FB50)	F001032 : Maintain fictitious GL account & hide activity via postings	Medium
Create Master Record (FS01) and Cash Journal (FBCJ)	F001033 : Maintain fictitious GL account & hide activity via postings	Medium
Create Master Record (FS01) and Enter Recurring Entry (FB01)	F001034 : Maintain fictitious GL account & hide activity via postings	Medium
Create Master Record (FS01) and Change Recurring Entry (FB02)	F001035 : Maintain fictitious GL account & hide activity via postings	Medium

**Figure 10** Risk Terminator Transaction Code Level Risk Analysis Report

If you click **Continue Role/Profile Assignment** the following prompt is displayed.



**Figure 11** Risk Terminator Warning

- 1 Click **Discard Changes** to discard any Role/Profile assignment to the user.
- 2 Click **Continue** to display the prompt as shown in [Figure 7](#).

When Role/Profile is Assigned to User(S) Using SU10

When you assign Role/Profile to User(s) using the **SU10** transaction and click **Save**, Risk Terminator checks for violations and if any are found, the report screen is displayed as shown next.

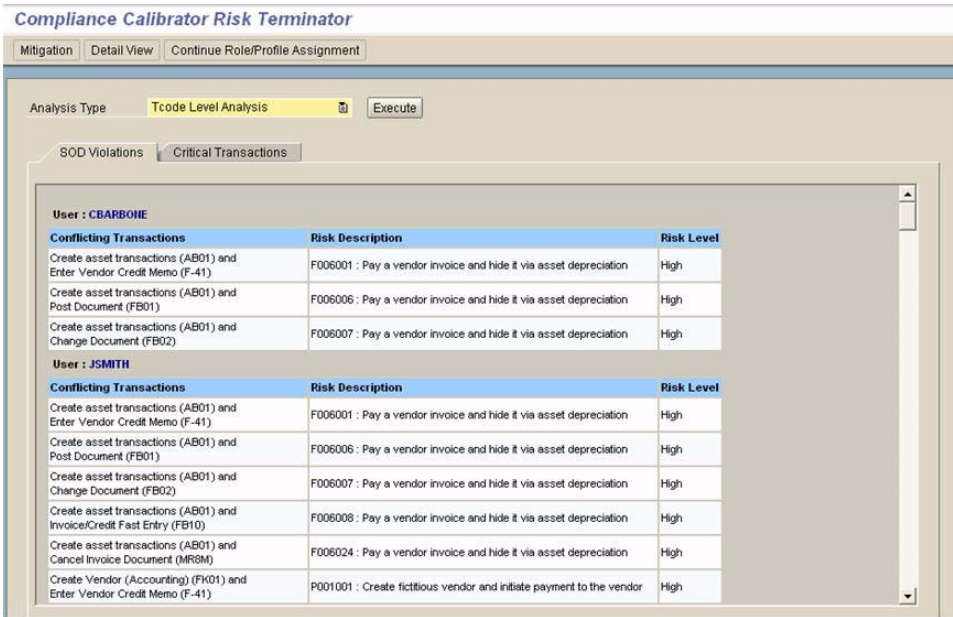


Figure 12 Risk Terminator Transaction Code Level Risk Analysis Report

If you click **Continue Role/Profile Assignment** the following prompt is displayed.



Figure 13 Risk Terminator Warning

- 1 Click **Discard Changes** to discard any Role/Profile assignment to the user.
- 2 Click **Continue** to display the prompt as shown in [Figure 7](#).

# 4

## RISK TERMINATOR LOG REPORTS

---

### TOPICS COVERED IN THIS CHAPTER

[Introduction](#)

# Introduction

The Risk Terminator Log report displays the log created when you enter reasons for generating a Role with SoDs.

To run this report type the following transaction code in the command field: /n/VIRSA/ZRTRGLOG.

### Risk Terminator Generation Log

Role	to	
User	to	
Generated By	to	
Generation Date	to	
Generation Time	00:00:00 to 00:00:00	

**Figure 14** Risk Terminator Log Report Form

Role User	Generated By	Generation Date	Generation Time	Reason
JSMITH	ManjitSingh Atwal(MANJIT)	06/20/2005	10:52:23	This role is required for GL and will be mitigated.

**Figure 15** Risk Terminator Log Report



# A

## INSTALLING RISK TERMINATOR

---

### TOPICS COVERED IN THIS APPENDIX

[Introduction](#)

# Introduction

Risk Terminator is an ABAP-based tool and is delivered to the customer as a group of transport files. This is the conventional delivery method for all add-on SAP software.

- Transport files are generally delivered in ZIP format. To install Risk Terminator, simply unzip and copy the Risk Terminator transport files on to your system.
- Please consult your Basis Administrator to install Risk Terminator in your system. Refer to OSS Note 13719 for more details on this procedure.
- If delivered with PAT files, Risk Terminator can be installed using the transaction SAINT. Unzip the PAT files and import into the system using the transaction SAINT.

Risk Terminator uses **PFCG** exits. You can also insert the following **SSM\_CUST** table entries manually using transaction **SM30**, as shown next:

Name	Value to be set
SAP_AFTER_PROF_GEN	WIRSAZ_AFTER_PROF_GEN
SAP_BEFORE_PROF_GEN	WIRSAZ_BEFORE_PROF_GEN
SAP_EXIT_USERS_SAVE	WIRSAZ_EXIT_USERS_SAVE

Figure 16 Table Maintenance

# B

## DELETING A ROLE LOCK

---

### TOPICS COVERED IN THIS APPENDIX

[Introduction](#)

---

## Introduction

On rare occasions, Risk Terminator prevents modifications to a Role by locking certain tables. You can use the following log utility to remove the lock and continue generating your Role.

Enter transaction code `/n/VIRSA/ZRTDELLOCK` , and enter the name of the Role.

The image shows a graphical user interface element for the Risk Terminator Log Utility. It consists of a light blue rectangular container. Inside, on the left, is the text 'Role' in a dark blue font. To the right of the text is a yellow rectangular input field with a thin blue border.

**Figure 17** Risk Terminator Log Utility