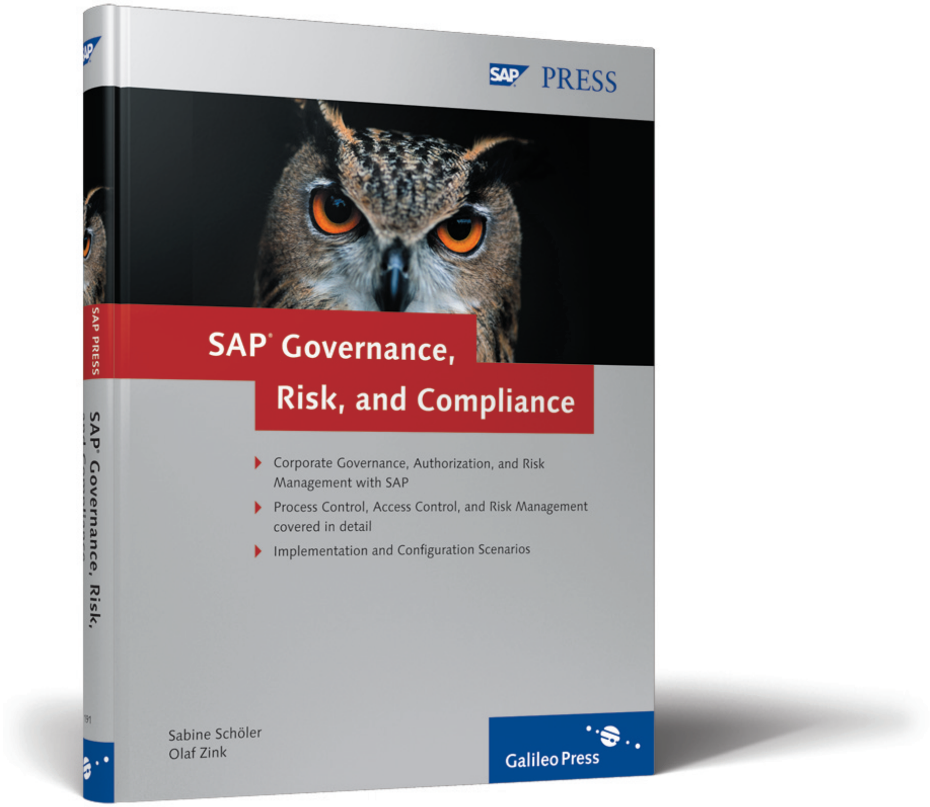
Sabine Schöler, Olaf Zink

SAP® Governance, Risk, and Compliance


SAP PRESS
SAP® Governance, Risk, and Compliance
Corporate Governance, Authorization, and Risk Management with SAP
Process Control, Access Control, and Risk Management covered in detail
Implementation and Configuration Scenarios
Sabine Schöler
Olaf Zink
Galileo Press

Galileo Press®

Bonn • Boston

Contents at a Glance

Contents

Two safety measures are better than one. (Cahier)

3 SAP GRC Access Control

SAP GRC Access Control provides a comprehensive range of functions to ensure that individual users within a corporation only receive the access rights they require for their daily work. As result related authorization risks will be detected, mitigated and prevented automatically. In this chapter, we describe the main application scenarios in detail and then present reporting options and configuration steps.

3.1 Overview of SAP GRC Access Control

How can we achieve complete compliance gradually in terms of the necessary separation of duties (SOD) in a corporation? How can we discover if user rights are being abused, and how do we avoid this in future? How can we reliably detect potential regulatory violations?? Using SAP GRC Access Control is the answer to these questions and therefore the solution for controlling access and authorizations in a corporation. SAP GRC Access Control consists of the following four business scenarios:

- **Risk Analysis and Remediation**
  Analyzes and remediates risks supporting an initial cleaning of the authorizations (Virsa Compliance Calibrator).
- **Enterprise Role Management**
  Manages enterprise roles during the design time of new roles (Virsa Role Expert).
- **Compliant User Provisioning**
  Performs compliant user provisioning so that no new violations are created with new user profiles (Virsa Access Enforcer).

- **Superuser Privilege Management**
  Manages superuser privileges for emergency access (Virsa Firefighter).

3.1.1 Access Risk Analysis and Remediation

Analyzing user data

In the *Access Risk Analysis and Remediation* application area, compliance with specifications that affect the segregation of duties (SOD) in the enterprise is supported in real time. Security controls should be prevented from being violated. In this case, the authorization assignments are first read and then analyzed in the connected SAP ERP systems. Risks are evaluated, the reason is detected, and the root cause can easily be resolved.

Adhering to the segregation of duties

When you evaluate read assigned authorizations, you use a rule set for the SOD. For example, if one and the same employee can create a vendor master record, trigger a purchase order, and initiate payment after an invoice has been received, this is regarded as a high risk. This comprehensive authorization profile means that the employee can invent a fictitious vendor and use regular business transactions to transfer company funds to an account. This would make it very easy for an employee with criminal intent to defraud the company.

Managing risks throughout the enterprise

You can use SAP GRC Access Control throughout the enterprise to find, evaluate, and correct violations of the SOD. In addition to SAP ERP systems you can also check applications from Oracle, PeopleSoft, JD Edwards, and Hyperion.

3.1.2 Enterprise Role Management (Virsa Role Expert)

SAP GRC Access Control already supports you when you design roles in the enterprise. The testing and maintenance phase follows the standardized and centralized design phase of roles. SAP GRC Access Control covers roles for the following business processes in SAP:

- Human resources
- Procure to pay
- Order to cash

- Finance (general accounting, project systems, fixed assets)
- Basis, security, and system administration
- Materials management
- Advanced Planning and Optimization (APO)
- Supplier Relationship Management (SRM)
- Customer Relationship Management (CRM)

Defining auditable roles

You can use SAP GRC Access Control to assign ownership for defining roles to business units. Role owners then define which activities and restrictions apply for the role. Therefore, they are subsequently also obliged to initiate approval processes for a role and use SAP GRC Access Control to store the history about changes made to roles. As another option, role owners can display the roles in which a certain transaction (e.g., triggering the payment run) was assigned. They can also compare different roles.

3.1.3 Compliant User Provisioning (Virsa Access Enforcer)

As jobs and responsibilities change in the enterprise, so too must the associated change in system authorizations be organized. New employees join the enterprise, and others leave. Areas of responsibility are redefined, or others are shared. SAP GRC Access Control supports you with the *Compliant User Provisioning (Virsa Access Enforcer)* function area by making it easier to process assigning and changing privileges and, at the same time, prevent any possible segregations of duties from being violated.

Automatic workflow for approval

If a job changes and, consequently, more comprehensive system access is also required, the employee makes this request himself by applying for the necessary profile through SAP GRC Access Control. The application triggers a workflow that is used to submit this change request to the employee's manager for approval.

Integration with SAP ERP HCM

You can also use an interface (*HR Real Time Agent*) to connect SAP GRC Access Control to SAP ERP Human Capital Management (SAP ERP HCM). Changes in the employee master record are managed by *infotypes* in the SAP ERP HCM application. You can use them to see whether an employee is leaving or joining the company, or whether his job profile has changed. The manager responsible is also displayed in the employee master record. You can use this interface to forward this HR-related information to SAP GRC Access Control and automatically notify the managers affected by the employee change. Notification occurs in the form of actions that are assigned to the managers or employees themselves. You'll learn more about using actions later in this chapter.

After you've requested the required authorization change, the possible effect is simulated. A check is carried out to see whether the rules set for the SOD will be violated if the request is approved.

SAP GRC Access Control enables the user to request the required authorization profiles without having to deal with the finer technical aspects in detail. The employee's manager can grant the access rights after he has used a simulation to assess the risk of the change. This reduces the workload of the IT department and means that it no longer has to discuss complex technical details of authorization profiles with the owners of the business units.

3.1.4 Superuser Privilege Management (Virsa Firefighter)

Assigning access rights in an emergency

In emergency situations, you can use SAP GRC Access Control to assign more access rights to end users than they normally require for their daily work. You do this by preparing a "Superuser" ID that is assigned to the user temporarily in an emergency.

All activities performed by the user under the "superuser" user ID are recorded and subsequently monitored and evaluated in detail.

3.1.5 Summary

Risk Analysis and Remediation

Figure 3.1 provides an overview of SAP GRC Access Control. The *Risk Analysis and Remediation* application area takes effect when you analyze the existing assignment of access rights for the first time after you've implemented SAP GRC Access Control. You also perform periodic checks of the SOD in the *Risk Analysis and Remediation* application area.

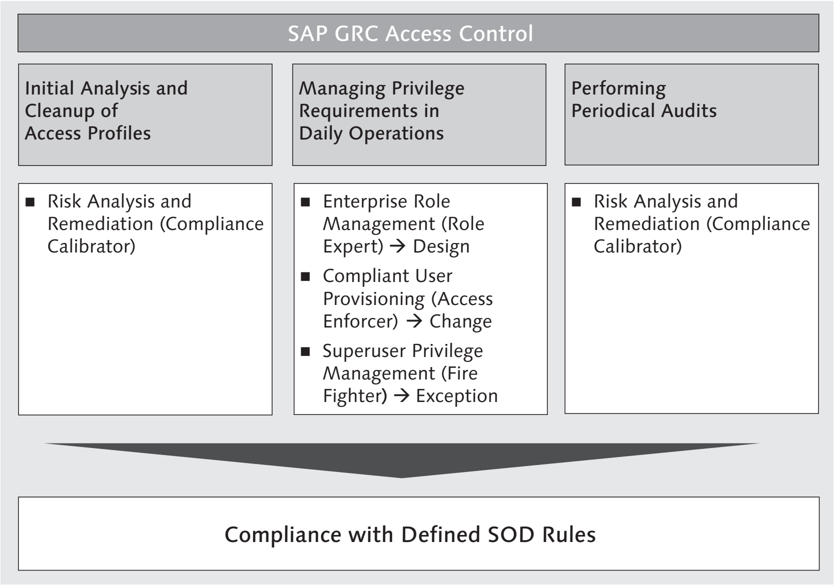

SAP GRC Access Control
Initial Analysis and Cleanup of Access Profiles
Managing Privilege Requirements in Daily Operations
Performing Periodical Audits
■ Risk Analysis and Remediation (Compliance Calibrator)
■ Enterprise Role Management (Role Expert) → Design
■ Compliant User Provisioning (Access Enforcer) → Change
■ Superuser Privilege Management (Fire Fighter) → Exception
■ Risk Analysis and Remediation (Compliance Calibrator)
Compliance with Defined SOD Rules

Figure 3.1 Overview of SAP GRC Access Control

To respond safely and with minimum risk to daily change requests for access rights, you use the other application areas of SAP GRC Access Control.

Enterprise Role Management

With Enterprise Role Management (Virsa Role Expert), you can already ensure that the required SOD is complied with when you design roles.

Compliant User Provisioning

If additional access rights are requested for a user profile, there is a risk that, due to this additional assignment of the authorization, the individual user will contain access rights that are too comprehensive from the point of view of SOD. This situation never occurs with *Compliant User Provisioning (Virsa Access Enforcer)* because the change is checked for possible risks before it's finally approved.

Superuser Privilege Management

In exceptional cases, users have to perform necessary repairs or have to perform important transactions. So they need emergency access without violating segregation of duties. This exceptional case is mapped using the *Superuser Privilege Management (Virsa Firefighter)* application area.

SAP GRC Access Control provides a comprehensive, cross-enterprise record of access controls that enables you to define coordinated roles throughout the enterprise and perform and monitor the SOD correctly. SAP GRC Access Control also provides enterprise-wide management in terms of defining and providing roles and of functions for privileged superusers.

3.2 Initial Analysis and Cleanup of Authorization Profiles

After we've successfully implemented SAP GRC Access Control for the EWP corporation, we first analyze the access rights assigned in the applications and IT systems. The objective is to find possible security and segregation of duties violations of errors in the authorizations assigned and any resulting risks for the enterprise.

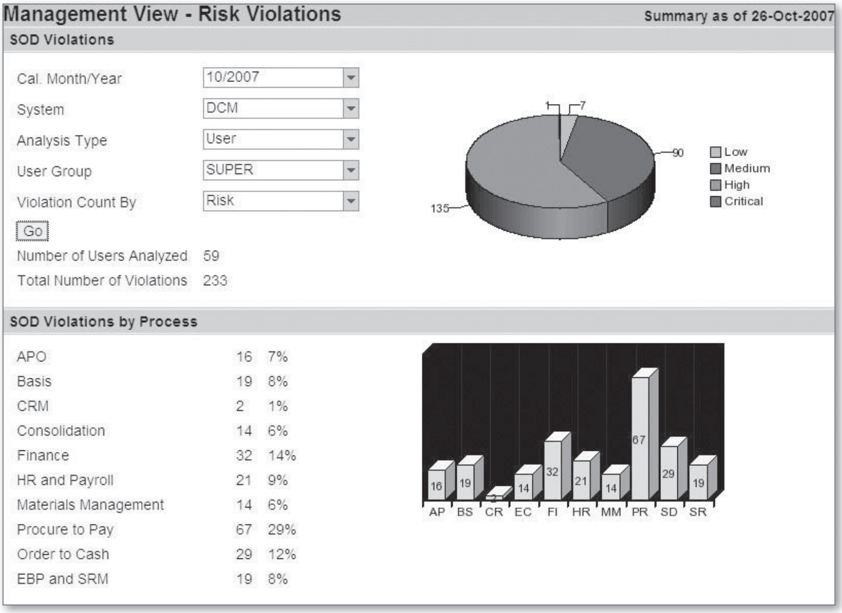
3.2.1 Identifying Risks

The starting point for reviewing the situation is the management overview of the authorization assignments that violate the rules for the segregation of duties (SOD). You obtain the analysis results by selecting the **Informer • Management View • Risk Violations** function path. The analysis results in Figure 3.2 show that **59** users were analyzed. The result of this analysis is **233** cases where the rules for the SOD were violated.

Management View

The **Management View** also provides information about how the identified risks are distributed on the different business processes. For example, **67** risks were identified in the **Procure to Pay** process.

By double-clicking the lettering of the **PR** column (procure to pay) in the lower-right section of the screen, you receive a list of risks that have been identified for the procure to pay business process.



Management View - Risk Violations

Summary as of 26-Oct-2007

SOD Violations

Cal. Month/Year	10/2007
System	DCM
Analysis Type	User
User Group	SUPER
Violation Count By	Risk

Go

Number of Users Analyzed 59

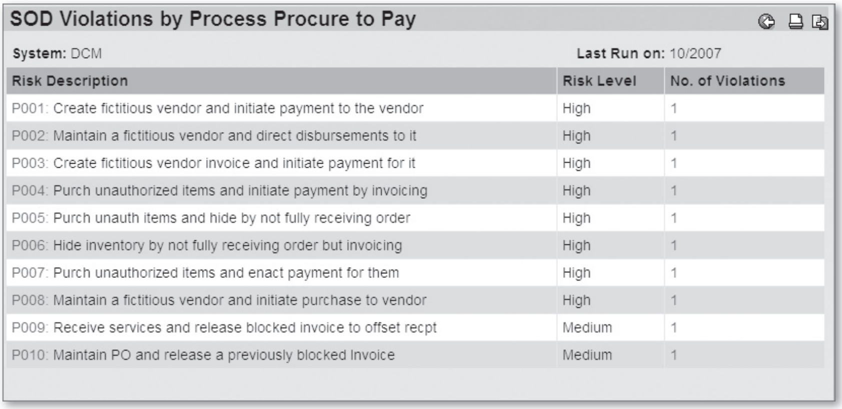
Total Number of Violations 233

SOD Violations by Process

APO	16	7%
Basis	19	8%
CRM	2	1%
Consolidation	14	6%
Finance	32	14%
HR and Payroll	21	9%
Materials Management	14	6%
Procure to Pay	67	29%
Order to Cash	29	12%
EBP and SRM	19	8%

Figure 3.2 Management View of Identified Risks

The numbers in the column on the right (see Figure 3.3) indicate how often the risks in question have been found. In this case, the risks have been identified for one user respectively.



SOD Violations by Process Procure to Pay

System: DCM **Last Run on:** 10/2007

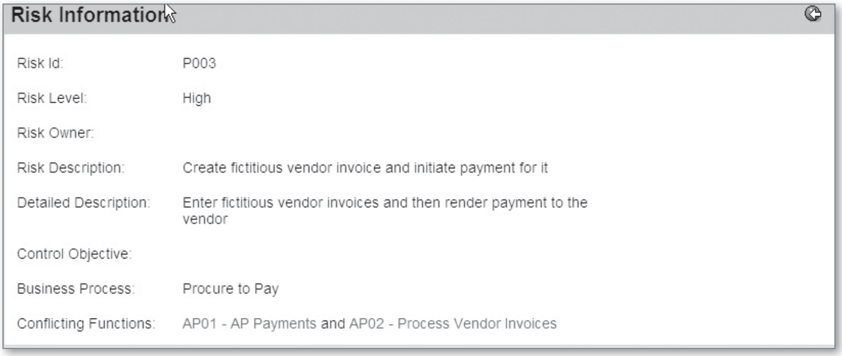
Risk Description	Risk Level	No. of Violations
P001: Create fictitious vendor and initiate payment to the vendor	High	1
P002: Maintain a fictitious vendor and direct disbursements to it	High	1
P003: Create fictitious vendor invoice and initiate payment for it	High	1
P004: Purch unauthorized items and initiate payment by invoicing	High	1
P005: Purch unauth items and hide by not fully receiving order	High	1
P006: Hide inventory by not fully receiving order but invoicing	High	1
P007: Purch unauthorized items and enact payment for them	High	1
P008: Maintain a fictitious vendor and initiate purchase to vendor	High	1
P009: Receive services and release blocked invoice to offset recpt	Medium	1
P010: Maintain PO and release a previously blocked Invoice	Medium	1

Figure 3.3 Overview of Risks for Procure to Pay Business Process

However, what exactly the risks involve is interesting for further analysis. The **P003** risk specifies that the user can create fictitious vendor invoices and also release payment for them. When you double-click the **P003** risk ID, the **Risk Information** window opens (see Figure 3.4).

Critical combination of functions

The risk information provides details about which critical combination of functions the user can execute. These are **AP01 - AP Payments** and **AP02 - Process Vendor Invoices** in the case presented here. This violates the rule for the SOD because a user should only execute one business function.



Risk Information

Risk Id:	P003
Risk Level:	High
Risk Owner:	
Risk Description:	Create fictitious vendor invoice and initiate payment for it
Detailed Description:	Enter fictitious vendor invoices and then render payment to the vendor
Control Objective:	
Business Process:	Procure to Pay
Conflicting Functions:	AP01 - AP Payments and AP02 - Process Vendor Invoices

Figure 3.4 Risk Information

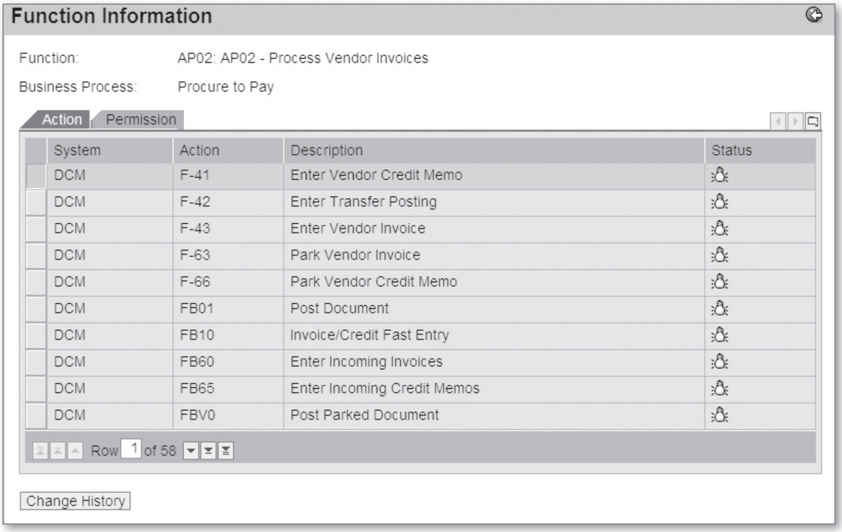
You can use the risk information to read the function conflicts at the business level. For the analysis, you don't need to know the technical details of the privilege concept.

Catalog of functions

SAP GRC Access Control has a catalog of functions that map the entire business processes of an enterprise. You can use the functions to bundle transactions and authorization objects. The bundling occurs in such a way that the rules for the SOD are complied with when you assign a function to a user.

If you want to check which transactions are assigned to the Process Vendor Invoices function, double-click the **AP02** function (Process Vendor Invoices).

There are 37 transactions assigned for the selected AP02 function (see Figure 3.5). Corresponding authorization objects are stored in these transactions (see Figure 3.6). You go to the list of authorization objects by selecting the **Permission** tab.



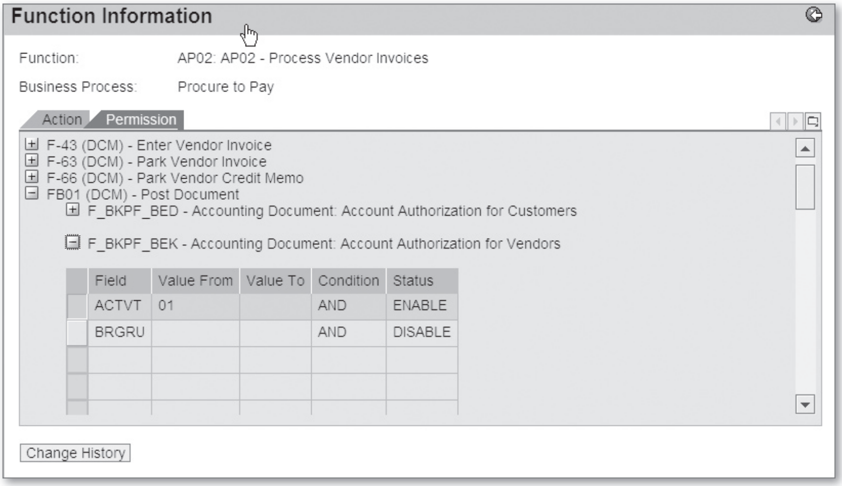
Function Information

Function: AP02: AP02 - Process Vendor Invoices

Business Process: Procure to Pay

System	Action	Description	Status
DCM	F-41	Enter Vendor Credit Memo	⚙
DCM	F-42	Enter Transfer Posting	⚙
DCM	F-43	Enter Vendor Invoice	⚙
DCM	F-63	Park Vendor Invoice	⚙
DCM	F-66	Park Vendor Credit Memo	⚙
DCM	FB01	Post Document	⚙
DCM	FB10	Invoice/Credit Fast Entry	⚙
DCM	FB60	Enter Incoming Invoices	⚙
DCM	FB65	Enter Incoming Credit Memos	⚙
DCM	FBV0	Post Parked Document	⚙

Figure 3.5 Function Information – List of Transactions



Function Information

Function: AP02: AP02 - Process Vendor Invoices

Business Process: Procure to Pay

- F-43 (DCM) - Enter Vendor Invoice
- F-63 (DCM) - Park Vendor Invoice
- F-66 (DCM) - Park Vendor Credit Memo
- FB01 (DCM) - Post Document
  - F_BKPF_BED - Accounting Document: Account Authorization for Customers
  - F_BKPF_BEK - Accounting Document: Account Authorization for Vendors

Field	Value From	Value To	Condition	Status
ACTVT	01		AND	ENABLE
BRGRU			AND	DISABLE

Figure 3.6 Function Information – List of Permission Objects

Risk rules

A catalog of risks, functions, and corresponding transactions and authentication objects is provided with SAP GRC Access Control. Possible combinations of authentication objects and transactions between two functions result in the list of risk rules (see Figure 3.7). SAP GRC Access Control provides over 100,000 risk rules, which, if they aren't observed, leads to a violation of the SOD and therefore represents a risk to the enterprise.

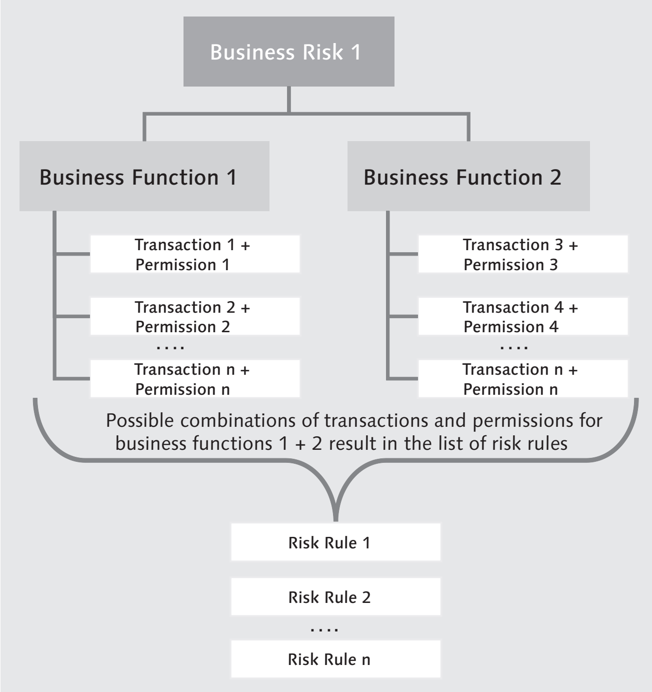

Business Risk 1
Business Function 1
Business Function 2
Transaction 1 + Permission 1
Transaction 2 + Permission 2
....
Transaction n + Permission n
Transaction 3 + Permission 3
Transaction 4 + Permission 4
....
Transaction n + Permission n
Possible combinations of transactions and permissions for business functions 1 + 2 result in the list of risk rules
Risk Rule 1
Risk Rule 2
....
Risk Rule n

Figure 3.7 Architecture of Risk Rules

Rule architect

You can use the rule architect to expand the list of risk rules in the course of the implementation.

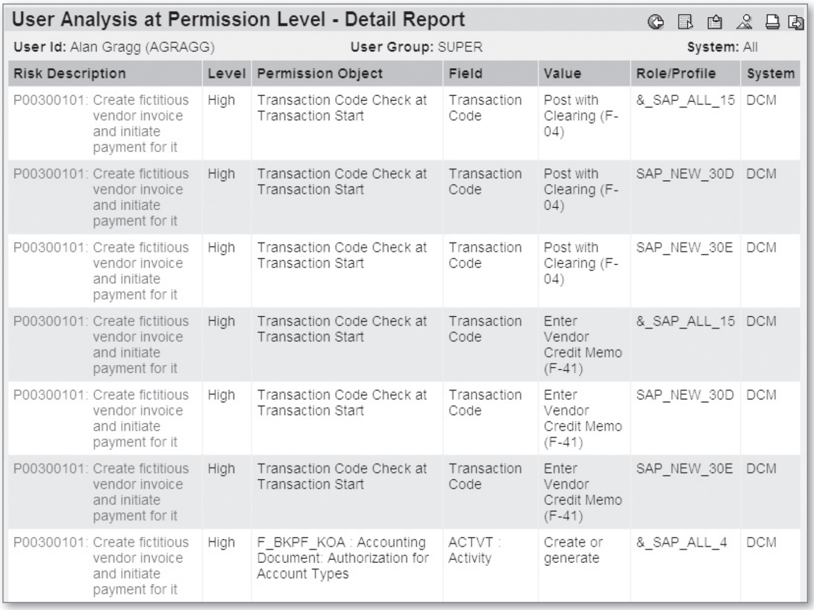
Business applications of third-party vendors

You can basically also connect ERP systems that aren't provided by SAP to SAP GRC Access Control. The data basis for functions and rules integrated into SAP GRC Access Control is also designed to read and evaluate permissions from business applications from Oracle, PeopleSoft, JD Edwards EnterpriseOne, and Hyperion. You can also connect your own applications (*legacy systems*) to SAP GRC Access Control. This approach enables you to check and improve compliance with the required SOD throughout the enterprise, even if an enterprise operates third-party business applications.

3.2.2 Cleaning Up Privilege Profiles

After the entire list of SOD violations has been made available, you must determine how to deal with this violation in each individual case.

According to the identified P003 risk, the accountant, Alan Gragg, has such extensive permissions that he could create fictitious vendor invoices and also release payment for them later (see Figure 3.8).



User Analysis at Permission Level - Detail Report

User Id: Alan Gragg (AGRAGG) User Group: SUPER System: All

Risk Description	Level	Permission Object	Field	Value	Role/Profile	System
P00300101: Create fictitious vendor invoice and initiate payment for it	High	Transaction Code Check at Transaction Start	Transaction Code	Post with Clearing (F-04)	&_SAP_ALL_15	DCM
P00300101: Create fictitious vendor invoice and initiate payment for it	High	Transaction Code Check at Transaction Start	Transaction Code	Post with Clearing (F-04)	SAP_NEW_30D	DCM
P00300101: Create fictitious vendor invoice and initiate payment for it	High	Transaction Code Check at Transaction Start	Transaction Code	Post with Clearing (F-04)	SAP_NEW_30E	DCM
P00300101: Create fictitious vendor invoice and initiate payment for it	High	Transaction Code Check at Transaction Start	Transaction Code	Enter Vendor Credit Memo (F-41)	&_SAP_ALL_15	DCM
P00300101: Create fictitious vendor invoice and initiate payment for it	High	Transaction Code Check at Transaction Start	Transaction Code	Enter Vendor Credit Memo (F-41)	SAP_NEW_30D	DCM
P00300101: Create fictitious vendor invoice and initiate payment for it	High	Transaction Code Check at Transaction Start	Transaction Code	Enter Vendor Credit Memo (F-41)	SAP_NEW_30E	DCM
P00300101: Create fictitious vendor invoice and initiate payment for it	High	F_BKPF_KOA : Accounting Document: Authorization for Account Types	ACTVT : Activity	Create or generate	&_SAP_ALL_4	DCM

Figure 3.8 User Analysis at Permission Level

You can call the detail report for the user analysis by choosing the **Informer • Risk Analysis • User Level** menu path. Select the *Detail* report format. This report displays the list of all violated risk rules at permission level.

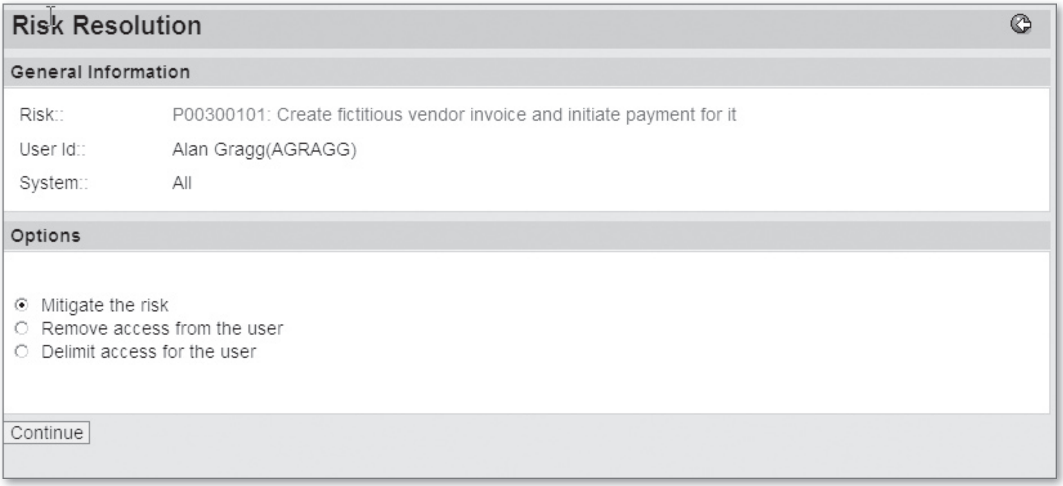
If you intend to process each violation of SOD individually, double-click to go to the ID number in the screen where you can specify how the risk is to be handled.

Options for handling risks

You can use the following three options here (see Figure 3.9):

- **Mitigate the risk**
  Reduce the risk for complying with access permission.

- **Remove access from the user**
  Remove access permission from the user completely.
- **Delimit access for the user**
  Temporarily limit access permission for the user.



Risk Resolution

General Information

Risk:: P00300101: Create fictitious vendor invoice and initiate payment for it

User Id:: Alan Gragg(AGRAGG)

System:: All

Options

● Mitigate the risk
○ Remove access from the user
○ Delimit access for the user

Figure 3.9 Risk Resolution

Mitigating the Risk for Complying with Access Permission

Mitigating the risk

You can create a control to mitigate the risk of comprehensive user permission for the enterprise. This can be so that a report is set up that performs a weekly check to see whether Alan Gragg (the user) has actually created a fictitious vendor and initiated a payment to the provider. A dual-control principle should also be established here. Tom Sanders, the second employee in Financial Accounting at EWP, has the task of checking the detailed payment run every month. If the report isn't requested by Tom Sanders every month through the payment run, the managing director, Andreas Schwarz, is notified of this via email.

Removing Access Permission from the User Completely

Removing access permission

In larger enterprises, users don't have an overview of which permissions have been granted to them over the years. The permissions are very often no longer adapted to meet the requirements of the current job or were created too comprehensively from the beginning. If the job description doesn't require the comprehensive permission, you can avoid the risk in this case by removing the access permission completely. At EWP, this means that Alan Gragg will no longer be able to create vendors or start payment runs in the future. To remove this permission for Alan Gragg, a work order is sent by workflow to the IT department following the decision by management to ensure that the mitigation of the permission can be technically implemented.

Temporarily Limit Access Permission for the User (Delimit Access for the User)

Delimiting access permission

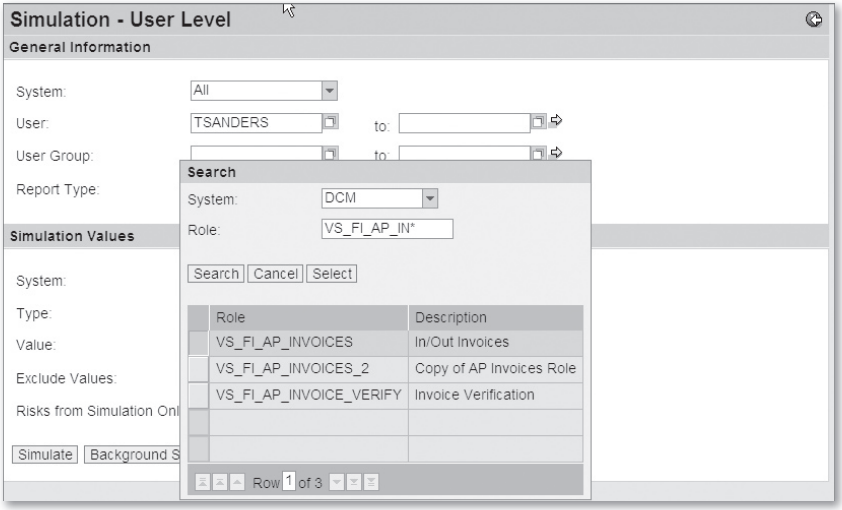
Temporarily limiting the assignment of permissions for a user is a useful way of mitigating risks if a basic solution is found in this time frame. At EWP, the division of work between Alan Gragg and Tom Sanders will essentially change within two months. After two months, Tom Sanders will take over vendor maintenance worldwide, and Alan Gragg will be responsible for the payment run worldwide. The *Create a Vendor Master Record* and *Initiate Payment Run* functions will therefore no longer be assigned to only one person. A SOD to two people will be successfully implemented. Here, the order for the technical implementation is also sent by workflow to the IT department, following approval by management.

Prevention through simulation

Setting up the SOD for Alan Gragg and Tom Sanders may cause other SOD violations.

To avoid issues here in advance, perform a simulation run before the actual technical implementation of the permission change by clicking the Simulate button when you call a report.

This enables you to simulate the assignment of other privileges to a user (see Figure 3.10), which means that you can rule out new risks from occurring for the entire enterprise by changing the privilege profile of individual employees.


Simulation - User Level

General Information

System: All

User: TSANDERS to:

User Group: to:

Report Type:

Simulation Values

System:

Type:

Value:

Exclude Values:

Risks from Simulation Onl

Search

System: DCM

Role: VS_FI_AP_IN*

Role	Description
VS_FI_AP_INVOICES	In/Out Invoices
VS_FI_AP_INVOICES_2	Copy of AP Invoices Role
VS_FI_AP_INVOICE_VERIFY	Invoice Verification

Row 1 of 3

Figure 3.10 Simulation at User Level

For large enterprises, after you perform this analysis for the first time, you'll get a high number of SOD violations. Compliance owners in the enterprise often have to resolve more than a million SOD violations. It's unrealistic to process every single violation. To deal with this type of situation, we recommend that you proceed as follows.

First, check the role concept, and resolve the existing SOD violations there within the roles and composite roles. Then, check whether certain roles can be removed for users, to ensure that the SOD is complied with throughout the enterprise.

Critical activities by Superuser Privilege Management

If you can't remove permissions for a user due to the size of the department, you can use Superuser Privilege Management to set up a specific user ID for critical activities (e.g., end-of-quarter closing). The employee then can perform the end-of-quarter closing under this special user ID, however, all of the work that the employee performs using this user ID will also be recorded down to the last detail.

If the options described previously are impractical, you can retain the critical permission assignment in individual cases. In this situation, however, you should ensure that the risk associated with this will be mitigated as much as possible. This can be done, for example, by another employee periodically creating and signing off on corresponding audit reports.

3.2.3 Preparing Audits

Preparing audits using reports

You can also use the reporting functions for the first-time analysis to prepare subsequent audits. The objective here is to obtain a regular overview of which risks exist due to SOD violations.

3.2.4 Rule Architect

SAP GRC Access Control provides a comprehensive combination of functions and associated rules for the SOD. This combination covers the following business processes of different business applications:

Rule architect – processes in the SAP system

Processes in the SAP System

- Human Capital Management (SAP ERP HCM)
- Procure to pay
- Order to cash
- Financials
  - General accounting
  - Project system
  - Fixed assets
- Basis, security, system administration
- Advanced Planning and Optimization
- Supplier Relationship Management(SAP SRM)
- Customer Relationship Management (SAP CRM)
- Consolidation

Rule architect – processes in the Oracle system

Processes in an Oracle System

- Human resources
- Procure to pay
- Order to cash
- Finance

    - General accounting
    - Project systems
    - Fixed assets
- System administration

Rule architect – processes in PeopleSoft

Processes in a PeopleSoft System

- Human resources
- Procure to pay
- Order to cash
- Finance
    - General accounting
    - Fixed assets
    - System administration

Rule architect – processes in JD Edwards

Processes in a JD Edwards System

- Human resources/payroll
- Procure to pay
- Order to cash
- Finance
    - General accounting
    - Consolidation

Rule architect – processes in Hyperion

Processes in a Hyperion System

- Custom rules

Enterprise-specific adjustment of rule set

You use the rule architect to extend the combination of rules and functions provided by SAP GRC Access Control. This consequently means that you can adjust the rule set to enterprise-specific requirements and also implement industry-specific extensions.

You also often have to connect application systems, which were developed by customers, to SAP GRC Access Control. In this situation, you use the rule architect to create customized functions and rules for customer development and then include them in the overall analysis.

Organization of enterprise

An important function in the rule architect is creating organization rules. You can use this function to store the organizational structure of the enterprise by mapping the company structure in detail. If an employee's privilege profile means that he can create fictitious vendor master records for a company and then allow a payment to this vendor, this is identified as a violation of SOD. However, the situation is different if the two functions *Create Vendor Master Record* and *Initiate Payment* affect different companies (different *company codes* in SAP terminology). The employee can create vendors within one company code and initiate the payment within another company code. Due to the organizational segregation of rules, this means that there is no longer a risk that the employee will transfer funds to a fictitious vendor.

3.3 Defining and Managing Roles

The basic objective is to plan possible roles in an enterprise so far ahead that SOD violations will be ruled out when you implement the roles in privilege profiles. This enables you to prevent any possible errors or fraud from the outset.

Employees from IT and the business unit can use *SAP GRC Access Control Enterprise Role Management* to jointly work out the best possible role structure for the enterprise. Each role is checked to see whether it violates the rules that an enterprise has established for achieving SOD. Obviously, this check is performed before the roles are released for use in a live system.

3.3.1 Defining Roles

Standardized method for designing roles

You can use SAP GRC Access Control to establish a standardized method for designing roles in the whole enterprise. A basic prerequisite for standardization is that you must follow the naming conventions for roles and profiles.

For example, you can specify that there should be a role in the enterprise that is to bundle the activities for processing the vendor master record. This consists of the following tasks in detail:

Index