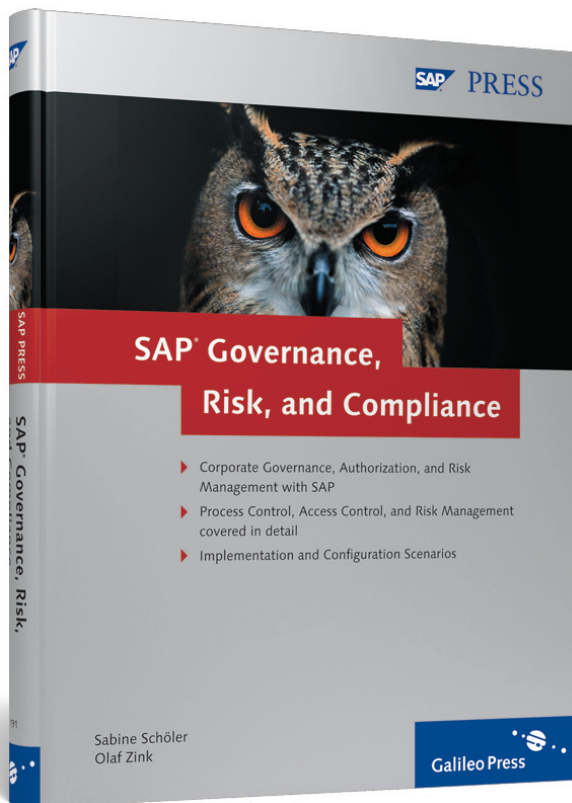


Sabine Schöler, Olaf Zink

SAP® Governance, Risk, and Compliance



 Galileo Press

Bonn • Boston

Contents at a Glance

1	Overview of SAP Solutions for Governance, Risk, and Compliance	15
2	SAP GRC Process Control	27
3	SAP GRC Access Control	101
4	SAP GRC Risk Management	203
5	SAP GRC Global Trade Services – An Overview	261
6	SAP Environment, Health & Safety – An Overview	281
7	An Outlook Ahead and a Product Roadmap	293

Contents

Introduction	11
1 Overview of SAP Solutions for Governance, Risk, and Compliance	15
1.1 Sample Company	15
1.2 Motivation and Goals of the GRC Project	17
2 SAP GRC Process Control	27
2.1 Objectives of SAP GRC Process Control	28
2.2 SAP GRC Process Control – Application	29
2.2.1 Organizational Structure	34
2.2.2 Assigning Processes at Organization Level	38
2.2.3 Assigning a Person to a Role	42
2.2.4 Creating and Planning a Survey	46
2.2.5 Performing Control Design Assessments	52
2.2.6 Automatic Tests	55
2.2.7 Analysis Dashboard and Reports	62
2.3 SAP GRC Process Control – System Configuration	68
2.3.1 Role Editing	70
2.3.2 Workflow	73
2.3.3 Structure	83
2.3.4 Automatic Testing and Monitoring	91
2.3.5 Reporting	94
3 SAP GRC Access Control	101
3.1 Overview of SAP GRC Access Control	101
3.1.1 Access Risk Analysis and Remediation	102
3.1.2 Enterprise Role Management (Virsa Role Expert) ...	102
3.1.3 Compliant User Provisioning (Virsa Access Enforcer)	103

3.1.4	Superuser Privilege Management (Virsa Firefighter)	104
3.1.5	Summary	104
3.2	Initial Analysis and Cleanup of Authorization Profiles	106
3.2.1	Identifying Risks	106
3.2.2	Cleaning Up Privilege Profiles	111
3.2.3	Preparing Audits	115
3.2.4	Rule Architect	115
3.3	Defining and Managing Roles	117
3.3.1	Defining Roles	117
3.3.2	Assigning Transactions and Authorizations to Roles	118
3.3.3	Performing Risk Analysis	120
3.3.4	Activities for Avoiding Risks	122
3.3.5	Deriving Roles	122
3.3.6	Approving Roles	123
3.3.7	Generating Roles	125
3.3.8	Mass Maintenance	125
3.4	Compliant User Provisioning	126
3.4.1	Requesting Self-Service Access Rights	127
3.4.2	Assigning Roles	128
3.4.3	Analyzing Risks and Approving Requests	129
3.4.4	Enterprise Application Systems	131
3.4.5	Saving Request History	131
3.5	Superuser Privilege Management	131
3.6	SAP GRC Access Control – Application and Configuration	136
3.6.1	Application and Configuration of Risk Analysis and Remediation	136
3.6.2	Overview of Configuration of the Enterprise Role Management Application Area (Virsa Role Expert)	166
3.6.3	Configuring the Compliant User Provisioning Application Area	181
3.6.4	Configuring the Superuser Privilege Management Application Area	193
3.6.5	Overview of Software Architecture	199
3.6.6	Technical How-to Guides	202

4 SAP GRC Risk Management 203

- 4.1 Goals of SAP GRC Risk Management 204
- 4.2 Business Processes in Risk Management 205
 - 4.2.1 Risk Planning – Enterprise-Wide Risk Management Approach 206
 - 4.2.2 Risk Identification and Analysis 207
 - 4.2.3 Risk Activities 208
 - 4.2.4 Risk Monitoring 208
- 4.3 User Roles 209
- 4.4 SAP GRC Risk Management – Application 211
 - 4.4.1 Risk Management Menu 212
 - 4.4.2 Organizational Unit 214
 - 4.4.3 Activities and Risk Catalogs 217
 - 4.4.4 Activities and Risk Documentation 220
 - 4.4.5 Risk Analysis With and Without a Response 228
 - 4.4.6 Risk Monitoring 231
- 4.5 SAP GRC Risk Management – System Configuration 234
 - 4.5.1 Setting Up a Transport Connection 236
 - 4.5.2 Creating the Top Node 237
 - 4.5.3 Configuring POWL 239
 - 4.5.4 Loss Event Database 247
 - 4.5.5 Workflow Activation 251

5 SAP GRC Global Trade Services – An Overview 261

- 5.1 Goals of SAP GRC Global Trade Services 261
- 5.2 S Legal Control 262
 - 5.2.1 Screening Sanctioned Party Lists 263
 - 5.2.2 Import/Export Control 266
- 5.3 Customs Management 269
- 5.4 Using Monetary Benefits and Limiting Monetary Risks ... 273
 - 5.4.1 Trade Preference Management (Preference Determination) 274
 - 5.4.2 Restitution Management (Refunds on Imports and Exports) 276
 - 5.4.3 Trade Finance Services (Documentary Payments Processing) 278

6 SAP Environment, Health & Safety – An Overview 281

6.1 Goals of SAP Environment, Health & Safety 281
6.2 Chemical Safety 282
6.3 Environmental Protection, Health Protection, and
Industrial Hygiene and Safety 285
6.4 Adherence to Product-Specific Environmental
Protection Regulations 289
6.5 Compliance Management and Emissions
Management 290

7 An Outlook Ahead and a Product Roadmap 293

7.1 Overview of 2008 and 2009 293
7.1.1 SAP Ramp-Up – The Product Launch Process
for SAP Solutions 293
7.1.2 SAP Solutions for Governance, Risk, and
Compliance – Status and Roadmap 295
7.2 Strategic Look Ahead After Integration with Business
Objects in SAP 297
7.2.1 Business Performance Optimization
Applications 298
7.2.2 Business Intelligence Platform 299

The Authors 301

Index 303

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 Fire-fighter).

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)

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.

Defining auditable 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.

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.

Automatic workflow for approval

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

Integration with SAP ERP HCM

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.

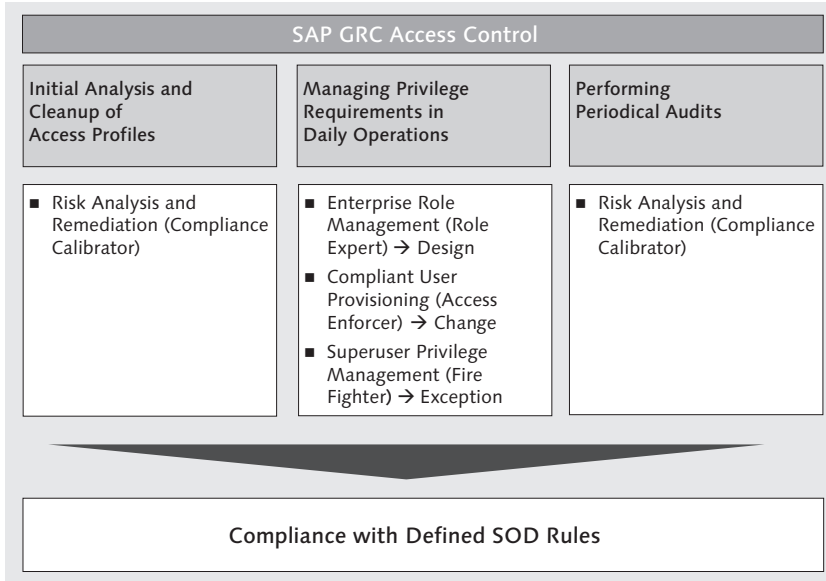


Figure 3.1 Overview of SAP GRC Access Control

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.

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

Enterprise Role Management

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.

Compliant User Provisioning

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.

Superuser Privilege Management

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.

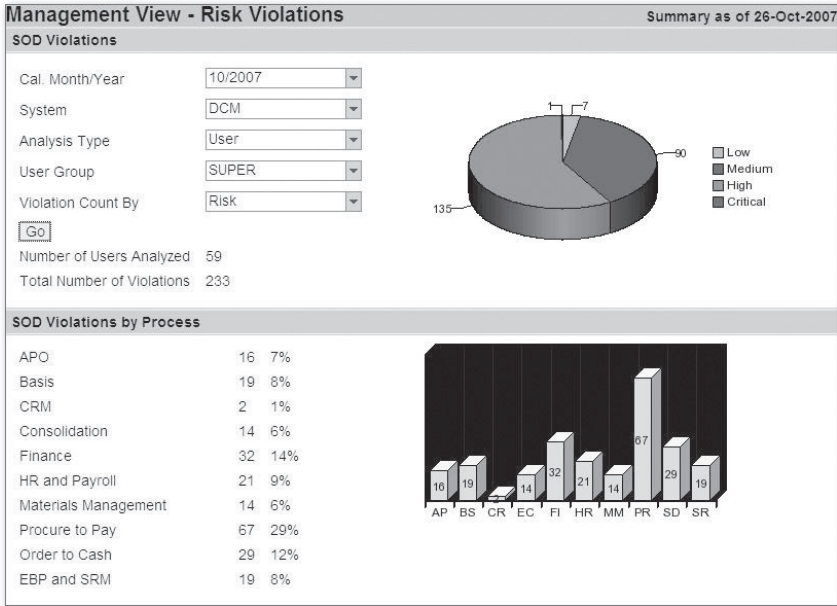


Figure 3.2 Management View of Identified Risks

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.

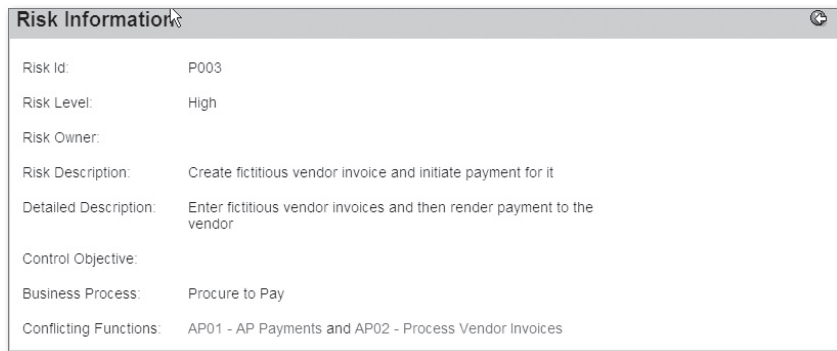


Figure 3.4 Risk Information

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.

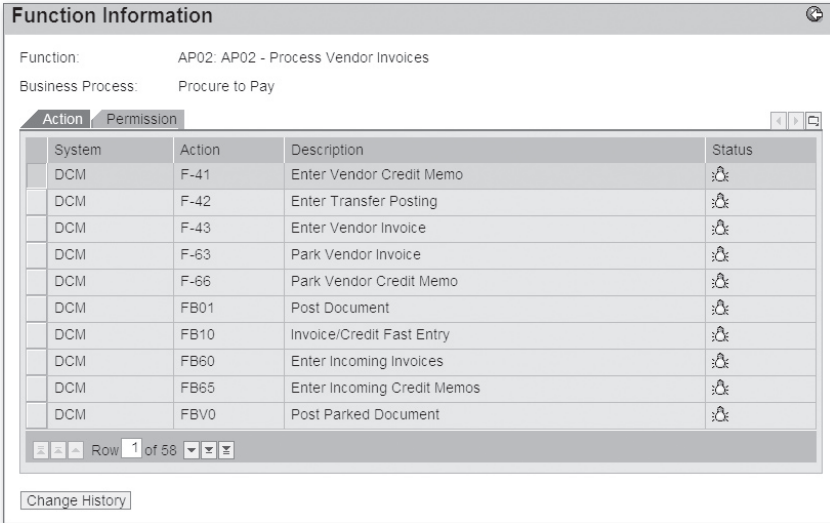


Figure 3.5 Function Information – List of Transactions

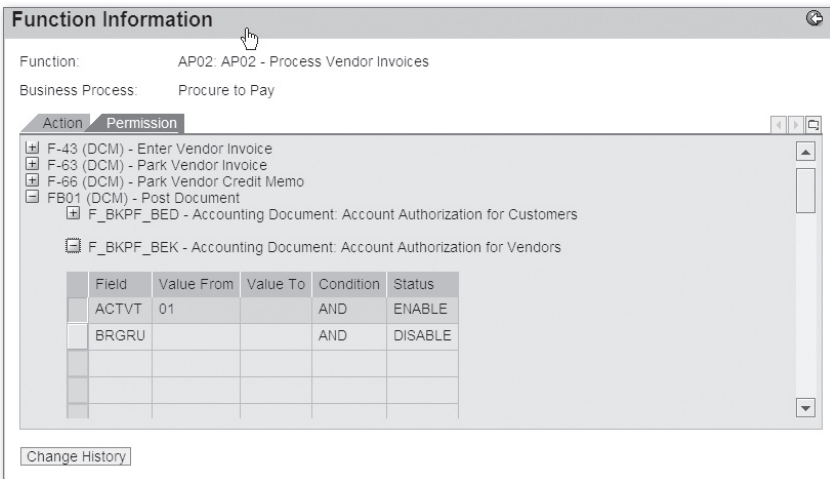


Figure 3.6 Function Information – List of Permission Objects

A catalog of risks, functions, and corresponding transactions and authentication objects is provided with SAP GRC Access Control. Possible com- Risk rules

binations 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.

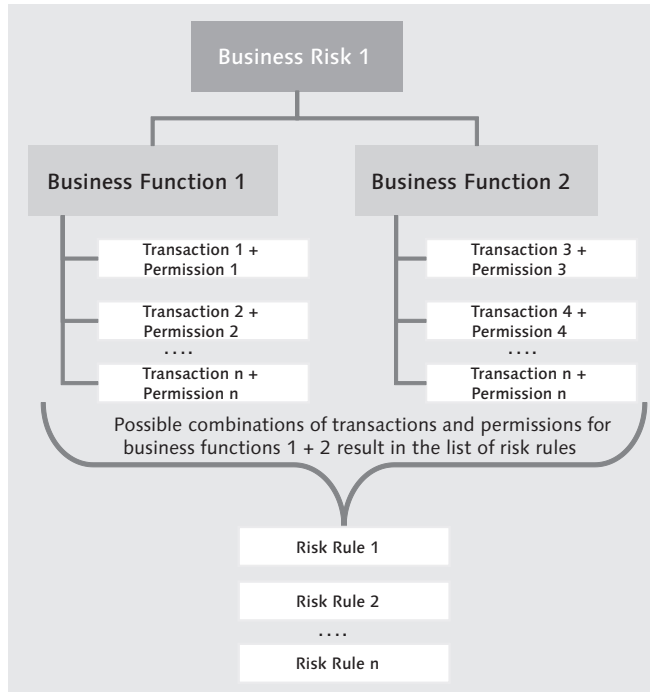


Figure 3.7 Architecture of Risk Rules

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.

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

► **Mitigate the risk**

Reduce the risk for complying with access permission.

Options for handling risks

- ▶ **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

Continue

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)

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.

Delimiting access permission

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

Prevention through simulation

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.

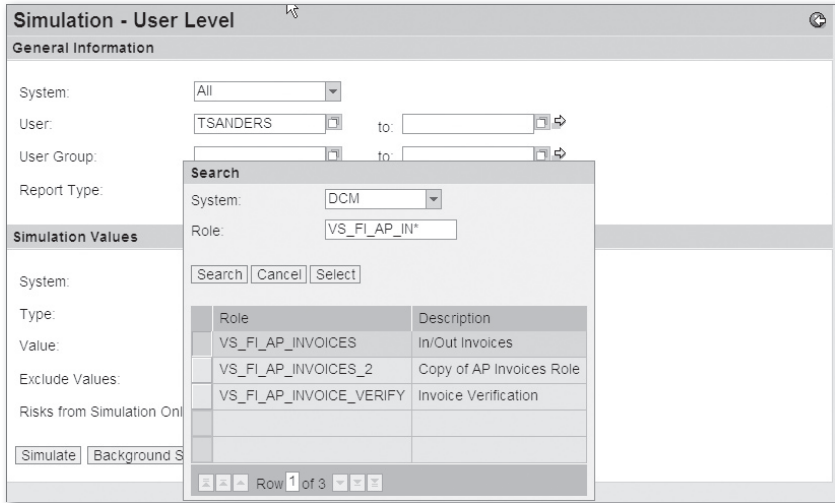


Figure 3.10 Simulation at User Level

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

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.

Preparing audits using reports

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:

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 SAP system

Processes in an Oracle System

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

Rule architect – processes in the Oracle system

- ▶ 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.

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.

Organization of
enterprise

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

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.

Standardized
method for
designing roles

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

A

- Accept risk, 224
- Access permission
 - Delimit*, 113
 - Mitigating the risk*, 112
 - Removal*, 112
- Access risk analysis and remediation, 101, 102
- Account, 30
- Action rule, 143
- Activate event linkage, 75
- Activities and risk catalogs, 217
- Activities catalog, 211, 218
- Activity, 217, 220
- Activity category, 218
- Activity groups, 218
- Adherence to product-specific environmental regulations, 282
- Administration program, 68, 98
- Administrator, 152, 181
 - Define*, 152
- Administrator rights, 152
- Advanced Planning and Optimization (APO), 103, 115
- Aggregation, 95
- Alert, 141, 155
- Alert monitor, 136
- Alert monitoring, 155
- Alternative recipient, 81
- A mitigation report was not initiated in the scheduled time interval., 136
- Analysis type, 57
- Analysis without Response, 225
- Analysis with Response, 229
- Analytics Dashboard, 30, 32, 60, 62, 63, 64
- Approval
 - Documentation*, 124
- Approval criteria
 - Search*, 178
 - Set up*, 178
- Approval process, 128
- Approval request, 124
- Assertion, 30
- Assessment, 53, 54
- Assessment and Test, 68, 89
- Assessment owner, 210, 221
- Assign agents, 253
- Assigning privileges in an emergency, 104
- Assigning rules to selected controls, 32
- Assigning the control rule, 58
- Assignment method, 39, 42
 - Copy*, 39
 - Reference*, 40
 - Without controls*, 40
- Assign persons to roles, 46
- Attribute, 68, 71
- Audit, 115, 131, 133
- Auditable role, 103
- Audit and Analysis, 33
- Auditor, 210
- Audit report, 137, 143
- Audit trail, 265
- Authentication
 - Configuration*, 185
- Authentication system, 185
- Automated control test, 28
- Automated test customizing, 32
- Automated test rule, 32
- Automatic control, 57, 59
- Automatic control monitoring, 55
- Automatic control rule, 59
- Automatic test, 55, 59, 60, 91
- Automatic transport connection, 69
- Automatic workflow Customizing, 73, 251
- Avoiding risks, 122

B

- Background job, 76, 199, 252
- Background job daemon, 162
- Background spool file, 163

- Blocked business partners, 264
 - Boycott lists, 262, 263
 - Business Add-In, 88, 94
 - Business Configuration Set (BC Set), 69
 - Business Intelligence Platform, 297
 - Business Objects company, 293
 - Business performance optimization
 - Applications*, 297
 - Business process
 - Create*, 147
 - Search*, 148
 - Business process owner, 204
 - Business unit
 - Define*, 152
- C**
-
- Case, 68
 - Case Management, 82
 - Category, 256
 - Central early warning system, 228
 - Centralized risk reporting, 208
 - Central permission assignment, 183
 - Central process catalog, 34
 - Central process hierarchy, 31
 - Central User Administration (CUA), 183, 184, 201
 - Certificate of origin, 276
 - Certification, 33
 - CFO cockpit, 293
 - CFO portfolio, 293
 - Chemical safety, 282
 - Classification, 271
 - Client, 237, 255
 - COBIT framework, 29, 60
 - Collaborative risk management scenario, 223
 - Company code, 117
 - Comparisons, 140
 - Complete overview, 204
 - Compliance, 17, 32, 62
 - Compliance Calibrator, 94
 - Compliance chart, 235
 - Compliance for Products (CfP), 289
 - Compliance management and emissions management, 282
 - Compliance structure, 30
 - Compliance test, 57, 59
 - Compliant User Provisioning, 101, 103, 105, 126
 - Configuration*, 181
 - integration*, 153
 - Concept of time-dependent definition, 36
 - Condition group
 - Create*, 174
 - Display*, 173
 - Set up*, 173
 - Configuration control, 56
 - Configure POWL, 239
 - Connector, 69, 91, 145, 168, 169
 - Configuration*, 181
 - Create*, 169
 - Consolidation, 115
 - Continuous transparency, 206
 - Control assessments, 65
 - Control automation, 50
 - Control design, 47, 48, 49, 52
 - Control design assessment, 49, 89, 90
 - Control documentation, 28
 - Control effectiveness, 55
 - Control monitoring, 32, 62
 - Control objective, 54
 - Control objectives and risks, 30
 - Control owner, 45, 53, 54, 63
 - Control rule assignment, 32
 - Controls Library, 142, 150
 - Corrective measure, 29
 - Cost-saving options, 61
 - Create top node, 239
 - Creating logs, 199
 - Critical combination of functions, 108
 - Critical profile, 149
 - Critical roles and profiles, 143
 - Current risk status, 211
 - Customizing for automatic test, 59
 - Customs clearance, 261
 - Customs documents, 272
 - Customs management, 269
 - Customs Management, 262
 - Customs tariff preference, 273
 - Customs value determination, 271

D

Dangerous goods check, 285
 Dashboard, 205, 212, 213
 Data extractor, 166
 DATA integration and data quality, 298
 DataSource, 97
 Deactivate linkage, 79
 Default query
 Define, 241
 Default Validator, 250
 Define category, 241
 Defining roles, 117, 176
 Delegation, 34
 Deriving roles, 122
 Detailed information, 137
 Dimension maintenance, 248
 Document, 35
 Documentary payments processing, 278
 Documentation, 284
 Documentation requirements, 199
 Document class, 98
 Document incident, 227
 Document Risk, 220
 Dual-control principle, 135

E

Email, 255
 Email server
 Set up, 187
 Embargo, 268
 Embargo checks, 262
 Embedded risk management, 204
 Emissions, 290
 Emissions certificates, 291
 Emissions Management, 290
 Enterprise Application System, 131
 Enterprise query, reporting, and analysis, 297
 Enterprise Role Management, 101, 102, 117, 122
 Configuration, 166
 Initial setup, 166
 Enterprise strategy, 204

Enterprise-wide process, 204
 Enterprise-wide risk identification, 205
 Enter vendor invoice, 120
 Entity-level control, 30, 34
 Entity-level control assessment, 49
 Environmental Protection, 285
 Environmental protection, health protection, and industrial hygiene and safety, 281, 282
 Environmental protection regulations, 289
 Escalation, 80
 Escalation procedure, 207
 Evaluation delay, 99
 Evaluation monitoring, 33
 Evaluation result, 32, 62
 Evaluation setup, 31, 56
 Event-based monitoring, 68, 99
 Event delivery, 77
 Event queue administration, 75
 Event start linkage, 78
 Excel template, 220
 Exception handling, 29
 Exclude expired users, 158
 Exclude locked users, 158
 Execution periodicity, 59
 Expert mode, 69, 84, 86
 Export license, 277
 Extractor, 200

F

Field group, 97
 Finance, 103, 115
 Financial Performance Management, 297
 Financials, 115
 Firefighter user ID, 104, 195, 198
 Firefighter (Virsa Firefighter), 198
 Firefight ID, 198
 Fixed assets, 103, 115
 Foreign trade regulations, 261
 Frequency of process, 50
 Frequency periods, 73
 Function
 Create, 146

Functional area
 Select, 119
Function information
 List of permission objects, 109
 List of transactions, 109

G

General accounting, 103, 115
Generating rules, 146
Generation of a role, 174
Global heatmap, 29
Goods import, 261
Governance management, 17
Governance, risk, and compliance (GRC), 15, 297
GRC maturity model, 21
Greenlight, 200

H

Hazardous substance management, 282
Hazardous substances, 284
Health Protection, 285
HR Real-Time Agent (RTA), 103
HR system, 185
HTTP, 96, 99
HTTP connection, 94
Human resources, 102, 115
Hyperion, 102, 110, 116, 165, 200

I

IBM Tivoli, 182
Identifying most efficient controls, 28
Identifying risks, 106
Identity management system, 201
Idle connection timeout, 160
Impact, 225, 230
Impact level, 215, 237
Import/export control, 262, 266
Import/export license, 268
Inbound Web Service, 93

Inbox, 52, 54
Index, 83, 94
Industrial hygiene and safety, 285, 286
Industrial hygiene and safety Data, 287
Informer, 136, 137
Initial data upload, 39, 220
Initial system data, 167
Interface, 201
Internal control manager, 36, 42, 44, 45, 52, 63, 68, 86
Internal controls, 52
Internal control system, 29, 42
Internal sanctioned party lists, 265
Issue, 54, 55, 62, 63, 97
Issue overview, 64
Issue owner, 55
Issue report, 89
Issue status, 66

J

J2EE database, 201
Java stack, 199
JD Edwards, 102, 110, 116, 131, 165, 200
Job monitor, 32

K

Key performance indicator (KPI), 209
Key risk indicator, 205

L

Labeling, 284
Labeling management function, 284
LDAP system, 185
Legacy system, 110, 165
Legal control, 262
Letter of credit, 278, 279
License, 266
Lightweight Directory Access Protocol (LDAP), 182

- List of controls, 151
- Local level, 40, 41
- Local master data, 37
- Logical port, 94
- Loss event database, 247
- Loss events, 209

M

- Maintain runtime environment, 73
- Management control, 30, 34, 49, 89
- Management View, 107, 137, 138
- Manually tested control, 31
- Manual test, 55, 59
- Manual Test Plan, 31
- Mass maintenance, 125
- Master data information, 201
- Master data services, 298
- Master data valid throughout the company, 37
- Material safety data sheets, 284
- Materials management, 103
- MDUG, 37, 69, 87
- Microsoft Active Directory, 182
- Mitigated risks, 158
- Mitigated users
 - List, 155*
- Mitigate the risk, 112
- Mitigating
 - Configuration, 186*
- Mitigating controls, 161
 - Create, 153*
 - Search monitors, 154*
- Mitigation, 136, 150
- Mitigation controls, 144
- Mitigation monitor, 150
- Monitoring, 32, 62
 - Controls, 55*
 - Of activities, 205*
- Monitoring control test, 57, 59
- Monitoring scheduler, 32
- My Home, 62, 212
- My Processes, 29

- My Tasks, 32, 62
- My Workflow Tasks, 29

N

- Naming conventions
 - Configure, 179*
 - Details, 179*
 - Set up, 178*
- New period, 83
- Notifiable transports, 284
- Notification, 245, 256, 258
 - Configuration, 190*
- Novell E-Directory, 182
- Number range, 83, 85, 99, 251
- Number range interval, 235
- NWBC settings, 68

O

- Object owner, 96
- Occupational health, 286
- Offline risk analysis, 160
- Oracle, 102, 110, 115, 131, 165, 200
- Oracle connectors, 182
- Order to cash, 102, 115
- Organization, 30, 34
- Organizational hierarchy, 36, 85, 87, 181
 - Edit, 36*
- Organizational structure, 34
- Organizational unit, 34, 214
- Organizational value mapping, 179, 180
- Organization owner, 63, 214, 238
- Organization rule, 117, 150, 160
- Organization-specific control, 40
- Org. level system parameter, 34
- Org-Level System Parameters, 32
- Overall assessment, 94
- Overdue assessment, 235

P

Password
 Set, 198
 PeopleSoft, 102, 110, 116, 131, 165, 200
 Performance, 83, 94
 Performance improvement, 75
 Performance increase, 79
 Performance problem, 96
 Permission level, 111
 Permission object, 108
 Personalization characteristics, 240
 Personalize, 67
 Personal Object Worklist (POWL), 81
 Personal worklist, 81
 Plan, 49, 50, 51
 Plan activity, 49
 Planner, 31, 59
 Planning, 57, 59
 Plant assets, 290
 Plant maintenance, 288
 Plant maintenance and repair measures, 288
 Preference determination, 274
 Preference processing, 274
 Preparing audits, 115
 Print report, 96
 Print Reports, 212
 Prioritization of subsequent responses, 205
 Privilege concept, 108
 Privileged users
 Superuser, 134
 Privilege profile, 106
 Cleaning up, 111
 Proactive monitoring, 208
 Proactive process, 204
 Proactive transparency, 228
 Probability level matrix, 243
 Probability levels, 242
 Probability of occurrence, 225
 Processes, 38
 Process vendor invoices, 108
 Procure to pay, 102, 106, 115
 Product classification, 266, 267, 270
 Product roadmap, 293

Product safety, 282
 Product-Specific Environmental Protection Regulations, 289
 Project system, 103, 115

Q

qRFC monitor, 79
 Quantitative risk analysis, 225
 Query, 32, 59
 Query visibility, 241
 Question category, 46
 Question Library, 46, 47
 Questions Library, 31

R

Ramp-Up process, 294
 Rating, 54
 Real-Time Agent (RTA), 199
 Reason code, 132
 Record table change, 69
 Refunds on imports and exports, 276
 Remediation, 54
 Remediation measure, 29, 32, 55, 62
 Remote Function Call (RFC), 197
 Remove access from the user, 112
 Report Center, 212, 232
 Reporting buffer, 95
 Reporting Center, 33, 62, 64
 Reporting type, 97
 Reports and Analytics, 30
 Request approval, 129
 Request for approval, 125, 129
 Request form, 127
 Request history, 131
 Requesting self-service permission access, 127
 Requirements of Section 404 of Sarbanes-Oxley Act, 28
 Residual risk, 231
 Response, 245
 Response activity, 220
 Response overview, 233

- Response owner, 210, 229, 230
- Response type, 246
- Response type combination, 247
- Restitution, 273, 277, 278
- Restitution management, 276
- Review required, 89
- Risk, 217, 220
 - Change history, 164*
 - Create, 147*
- Risk activity, 205, 208
- Risk analysis, 137, 142, 143, 207, 220, 225, 228, 241
 - Additional options, 161*
 - Default report type, 157*
 - Default risk level, 157*
 - Default rule set, 158*
 - Default settings, 159*
 - Default user type, 158*
 - Perform, 129*
 - Performance tuning, 159*
 - Performing, 120*
 - Start, 121*
- Risk Analysis and Remediation, 101, 136
- Risk analysis with a response, 228
- Risk analysis without a response option, 225
- Risk Assessment, 212, 220
- Risk catalog, 207, 211
- Risk category, 219
- Risk dependencies, 204
- Risk documentation, 222, 223, 225
- Risk group, 219
- Risk hierarchy, 219
- Risk identification, 204, 207
- Risk information, 108, 164
- Risk level, 225, 244
- Risk level ID, 244
- Risk level matrix, 244
- Risk management, 17
- Risk management response, 229, 231
- Risk manager, 209, 212, 214, 216
- Risk monitoring, 206, 208, 231
- Risk owner, 210, 222, 223
- Risk planning, 205, 206
- Risk prevention, 205
- Risk priority, 225, 245
- Risk priority ID, 245
- Risk priority matrix, 245, 246
- Risk profile, 204, 205
- Risk propensity, 205
- Risk remediation, 112
- Risk response, 205, 208, 232, 233, 246
- Risk response strategy, 246
- Risk revaluation, 245
- Risk rule, 109, 110
 - Architecture, 110*
- Risk situation, 232
- Risk status, 227
- Risk Structure, 212
- Risk threshold, 215
- Risk tolerance, 207
- Risk validator, 211, 221
- Risk violations, 138
- Role, 34, 35, 70, 114, 209, 211, 214
 - Administrator, 194*
 - Approve, 123, 174*
 - Assign, 34, 46, 128, 196*
 - Authorization, 33*
 - Controller, 194*
 - Create, 118*
 - Critical, 149*
 - Editing, 70*
 - Firefighter user, 194*
 - For subprocess, 44*
 - Generate, 125*
 - Owner, 194*
 - Task, 34, 35, 42*
- Role analysis, 139
- Role attribute, 170
 - Business process, 171*
 - Custom fields, 172*
 - Functional area, 172*
 - Project/release, 173*
 - Set up, 170*
 - Subprocess, 171*
- Role-based dashboards, 208
- Role catalog, 128
- Role concept, 114
- Role definition, 117
 - Methodology, 174*
- Role details, 128
- Role ID, 70
- Role level, 44

- Role management, 117
 - Role type, 81
 - Root organizational unit, 238
 - Rule, 32, 56, 92
 - Rule architect, 110, 115, 116, 120, 136, 145, 148
 - Processes in Hyperion, 116*
 - Processes in JD Edwards, 116*
 - Processes in Oracle system, 115*
 - Processes in Peoplesoft, 116*
 - Processes in SAP system, 115*
 - Rule configuration, 32
 - Rule criteria, 32, 56, 57
 - Rule criterion, 57
 - Rule definition, 56
 - Rule groups, 92
 - Rule parameter, 56, 57
 - Rule script, 32
 - Rule set, 148
 - Create, 149*
 - Search, 149*
 - Rules Library, 141, 145
 - Runtime environment, 251
- S**
-
- Sanctioned party lists, 263
 - Sanctioned party list screening, 264
 - SAP_ALL, 131
 - SAP Business Information Warehouse, 97
 - SAPconnect communication interface, 81
 - SAP connector, 182, 183
 - SAP Corporate Services, 288
 - SAP Customer Relationship Management (SAP CRM), 103, 115
 - SAP Development Network (SDN), 202
 - SAP Enterprise Asset Management, 288
 - SAP Environmental Compliance, 290
 - SAP Environment, Health & Safety (SAP EH&S), 25, 281
 - SAP ERP Financials, 291
 - SAP ERP Human Capital Management (SAP ERP HCM), 103, 115, 288
 - SAP GRC Access Control, 24, 94, 101
 - Application, 136*
 - Configuration, 136*
 - SAP GRC Applications Integration Documentation, 167
 - SAP GRC Global Trade Services, 25, 261
 - SAP GRC Process Control, 25
 - SAP GRC Risk Management, 25
 - Configuration, 234*
 - SAP NetWeaver, 200
 - SAP NetWeaver Business Client, 99
 - SAP NetWeaver Business Intelligence (SAP NetWeaver BI), 201
 - SAP NetWeaver Identity Management, 201
 - SAP Product Lifecycle Management (SAP PLM), 291
 - SAP Supplier Relationship Management (SAP SRM), 103, 115
 - SAP Supply Chain Management, 291
 - SAP System Landscape Directory (SLD), 183
 - SAP User Management Engine (UME), 185, 200
 - Sarbanes-Oxley Act (SOX), 42
 - Scheduling, 32, 59
 - Scheduling frequency, 73
 - Scheduling function, 83
 - Script, 56, 57
 - Script category, 56
 - Script type, 56
 - Section 302
 - Sarbanes-Oxley Act (SOX), 29*
 - Security configuration, 191
 - Security report, 137, 144
 - Segment dimension, 248
 - Segment table, 247, 250
 - Segment table operation, 250
 - Segment tables list, 249
 - Segregation of duties (SOD), 101, 102, 106
 - Selection, 256
 - Selection procedure, 50
 - Self-assessment, 31, 49
 - Sequential processing of events, 78
 - Server performance, 99
 - Set Default Corporate ID, 239
 - Set up structure, 84

Shared Objects Memory, 87
 Shared Services Provider, 34, 40
 Siebel, 165
 Significant deficiency, 54
 Sign-off, 31, 34, 36, 49, 64, 83, 97
 Sign-off monitor, 33
 Sign-off process, 31
 Simulation, 113
 At user level, 114
 SLD connector, 183
 SMTP server, 187
 Software architecture, 200
 Specification database, 282
 Stage configuration, 188
 Standard evaluation report, 33
 Standard SAP report, 32, 59
 Standard SAP workflow function, 29
 Standard task, 73, 253
 Start of receivers, 77
 Structure, 68
 Structure and Setup, 33
 Subprocess, 34, 38
 Assign, 38
 Assign to Organization, 42
 Financial reporting, 171
 General ledger, 171
 Subprocess design, 49
 Subscription, 258
 Substitute, 34
 Successor, 34, 80
 Sun Microsystems SunOne, 182
 Superuser, 134
 Report, 135
 Superuser Privilege Management, 102, 104, 105, 114, 131, 132, 193
 Superuser Privilege Management roles, 195
 Supported languages, 83
 Survey, 31, 46, 47, 49, 52, 255
 Survey category, 47
 Survey Library, 31, 47, 48
 Sustainability reports, 290
 System administration, 103, 115
 System connections, 165
 System landscape, 169
 Create, 170
 Define, 168

System performance, 67, 87
 System type, 56, 91

T

Target attribute, 239
 Task number, 257
 Task-specific Customizing, 75, 253
 Technical how-to guides, 202
 Test automation, 50
 Tester, 45
 Third-party provider, 165
 Third-party vendor, 110, 111
 Three point analysis, 242
 Threshold value, 238
 Time frame, 242
 Timeout, 160
 Tolerance values, 57
 Top node, 237
 Top organizational unit, 238
 Tracking the cause, 233
 Trade Finance Services, 278
 Trade Preference Management, 274
 Transaction, 108
 Assign, 118
 Transparency, 204
 Transparent information, 205
 Transport request, 92
 Trigger warning message, 226

U

Uniform platform, 204
 Universal Description, Discovery, and Integration (UDDI), 93
 URL links, 35
 User access, 34, 35
 User analysis, 111, 138, 139
 User data source
 Define, 185
 User-defined field, 68, 88
 User ID, 133, 199
 User maintenance, 195
 User roles, 209

User synchronization, 159

V

Validate risk, 224

Validation, 90, 250

Validation indicator, 249

Vendor invoice, 150

Vendor maintenance, 133

Vendor master record, 120, 121

Change, 118

Create, 118

Delete, 118

Lock, 118

Maintain, 122

Virsa Access Enforcer, 101, 103

Virsa Compliance Calibrator, 101

Virsa Firefighter, 73, 102, 104, 131, 134

Virsa Role Expert, 102, 166

Visualization and reporting, 297

Web Service, 99, 201

Web Service worker threads, 159

Workflow, 73, 98, 128, 162

Approval criteria, 177

Workflow activation, 251

Workflow function, 211, 223, 251, 255

Workflow initiator

Create, 187

Workflow path

Create, 192

Details, 193

Set up, 192

Workflow sample, 73

Workflow stages

Create, 188

Workflow task, 52, 54

Workflow template, 253

Workflow with errors, 76

Work inbox, 29, 52, 224

Worklist Type, 240

Worklist Type Repository, 240

W

Warning message, 205

Waste disposal, 285