Raj Behera

Cross-Enterprise Integration with SAP® GRC Access Control

Galileo Press
Bonn • Boston
# Contents

1 Introduction ............................................................................................... 9

1.1 What is Access Control? ................................................................. 9
   1.1.1 Risk Analysis and Remediation (RAR) ............................ 10
   1.1.2 Protect Information and Prevent Fraud .......................... 12

1.2 Architecture of Access Control ................................................................ 13

1.3 Necessity of SOX ............................................................................... 15

1.4 Overview of Cross-Enterprise for Access Control .............................. 18

1.5 Summary ......................................................................................... 19

2 SAP GRC Access Control Rule Architect ........................................... 21

2.1 Overview of the Rule Architect ....................................................... 21
   2.1.1 Rule Files ......................................................................... 23
   2.1.2 How to Create Rules in an Application ............................ 35
   2.1.3 Active Rules ..................................................................... 37
   2.1.4 Rule Architect Dashboard ................................................. 41

2.2 Building Cross-Enterprise Rules ....................................................... 43
   2.2.1 Example ........................................................................... 44

2.3 Summary ......................................................................................... 45

3 Managing Access Risk ........................................................................... 47

3.1 Central Rule Library: The Global Rule Set ....................................... 47
   3.1.1 Risk Recognition ............................................................... 48
   3.1.2 Risk Identification ............................................................ 48

3.2 Rule Migration in the System Landscape and During the RAR Upgrade Process ......................................................... 48

3.3 Import/Export Utility .......................................................................... 50
   3.3.1 Configuration .................................................................... 50
   3.3.2 Features ........................................................................... 51

3.4 Summary ......................................................................................... 55
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Cross-Enterprise Matrix for SAP GRC AC</td>
<td>57</td>
</tr>
<tr>
<td>4.1</td>
<td>Available Real Time Agent (RTA) for SAP</td>
<td>57</td>
</tr>
<tr>
<td>4.2</td>
<td>RTA for Non-SAP ERP Applications</td>
<td>58</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Integration with Oracle</td>
<td>59</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Integration with PeopleSoft</td>
<td>63</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Integration with JDE</td>
<td>63</td>
</tr>
<tr>
<td>4.2.4</td>
<td>Integration with Legacy Systems</td>
<td>64</td>
</tr>
<tr>
<td>4.2.5</td>
<td>RTA Deployment</td>
<td>64</td>
</tr>
<tr>
<td>4.2.6</td>
<td>Connector Creation</td>
<td>64</td>
</tr>
<tr>
<td>4.3</td>
<td>Summary</td>
<td>64</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Configuration and Operation of the Data Extractor</td>
<td>65</td>
</tr>
<tr>
<td>5.1</td>
<td>System Connector</td>
<td>67</td>
</tr>
<tr>
<td>5.2</td>
<td>Configure Extraction Process</td>
<td>67</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Extraction Process in Legacy Systems</td>
<td>68</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Extraction Process in SAP Access Control</td>
<td>70</td>
</tr>
<tr>
<td>5.3</td>
<td>Production</td>
<td>80</td>
</tr>
<tr>
<td>5.4</td>
<td>Summary</td>
<td>80</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Risk Analysis for Cross-Enterprise Systems</td>
<td>81</td>
</tr>
<tr>
<td>6.1</td>
<td>Scheduling Background Jobs</td>
<td>81</td>
</tr>
<tr>
<td>6.1.1</td>
<td>Scheduling Synchronization Jobs, Including Methods for Legacy/Offline Systems</td>
<td>82</td>
</tr>
<tr>
<td>6.1.2</td>
<td>Scheduling Batch Risk Analysis</td>
<td>84</td>
</tr>
<tr>
<td>6.2</td>
<td>Management Report Updates</td>
<td>85</td>
</tr>
<tr>
<td>6.3</td>
<td>Real Time Risk Analysis</td>
<td>86</td>
</tr>
<tr>
<td>6.4</td>
<td>Cross-Enterprise Execution in the AC Application</td>
<td>87</td>
</tr>
<tr>
<td>6.5</td>
<td>Offline Risk Analysis</td>
<td>92</td>
</tr>
<tr>
<td>6.6</td>
<td>Summary</td>
<td>93</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Mitigation and Alerts</td>
<td>95</td>
</tr>
<tr>
<td>7.1</td>
<td>Mitigation Controls</td>
<td>95</td>
</tr>
<tr>
<td>7.2</td>
<td>Mitigated Users/Roles/Profiles/HR Objects</td>
<td>96</td>
</tr>
<tr>
<td>7.2.1</td>
<td>How to Create a Mitigation Control</td>
<td>96</td>
</tr>
</tbody>
</table>
Contents

7.3 Alert Generation ................................................................. 101
7.4 Alert Dashboard ................................................................. 103
7.5 Alert Clearing and Archiving ........................................... 104
7.6 Summary ........................................................................... 105

8 Continuous Compliance ..................................................... 107

8.1 Best Practices for Continuous Compliance ....................... 107
8.2 Simulation ......................................................................... 109
8.3 Monitoring and Control .................................................... 112
8.4 Summary ........................................................................... 112

Appendices ............................................................................. 113

A Rule Library File Templates ............................................... 115
A.1 Business Process Template ............................................. 115
A.2 Function Template .......................................................... 115
A.3 Function-Business Process Relationship Template ........... 116
A.4 Function-Action Relationship Template ............................ 116
A.5 Function-Permission Relationship Template ..................... 116
A.6 Rule Set Template ........................................................... 117
A.7 Risk Definition Template ................................................ 117
A.8 Risk Description Template ................................................ 118
A.9 Risk to Rule Set Relationship Template ............................. 119

B Legacy System Templates ..................................................... 121
B.1 User File Template ............................................................ 121
B.2 User Action File Template ............................................... 122
B.3 User Permission File Template ......................................... 122
B.4 Role File Template ............................................................ 124
B.5 Role Action File Template ................................................ 124
B.6 Role Permission File Template ......................................... 125
B.7 Profile File Template .......................................................... 126
B.8 Profile Action File Template ............................................. 126
B.9 Profile Permission File Template ...................................... 127
B.10 Action File Template ........................................................ 127
B.11 Permission File Template ................................................. 128
B.12 Field File Template .......................................................... 129
B.13 Value File Template ........................................................ 130
Contents

C Information Sources ............................................................................................. 133
  C.1 Installation and Upgrades ........................................................................ 133
  C.2 SAP Help Portal for Access Control ..................................................... 134
D The Author ...................................................................................................... 135

Index .................................................................................................................. 137
This chapter discusses changes in roles and user assignments, and shows you how to simulate changes to roles and users. It also shows you how to implement alerts to monitor for newly selected risks and mitigating control testing. In addition, it provides details on how to provide continuous compliance throughout the year, including a few tips and tricks to manage the cross-enterprise project.

8 Continuous Compliance

Continuous compliance can be achieved through preventive control mechanisms, 24/7 monitoring functions, adoption of proactive compliance, and cross-enterprise risk analysis. The ability to have compliance across the organization depends on an effective monitoring, simulation, and remediation plan. SAP GRC AC offers various attributes to make it compliant, including detection solution, alerts, simulation, preventive analysis, real time risk analysis, integration models for cross-enterprise systems, and more.

8.1 Best Practices for Continuous Compliance

The list that follows outlines the steps necessary to achieve continuous compliance:

1. Review your risk statement and its impact on the SoD analysis to gain a better understanding of the risk recognition and mitigation approach.

2. Review the system configuration for the risk impacts to the enterprise. Perform the necessary steps to avoid conflicting action issues and validate the system security for multiple access control systems.

3. If the management report provides a variety of SoD violations, critical actions, or critical permissions, it is advisable to take corrective action and remove high usage roles from users.
4. Maintain continuous monitoring of the object values within roles and their impacts—object authorization can be a potential problem to the role design. By introducing an effective simulation process, these problems can be avoided.

5. Design other preventative controls via system configuration; for example, arrange certain objects and transaction codes to better determine critical violations.

6. If a preventative control is failing, create an effective method for monitoring the control within organizations across enterprises. This could include file monitoring, report verification, alert control monitoring, process design review, central rule library maintenance, or workflow.

In short, you need to develop a report that provides accurate data for reviewers. For example, an SAP report exists that shows whether a user performs a goods receipt against a purchase order he created. This report needs to be reviewed on a scheduled periodic basis, and its accuracy should be verified for audit purposes. If the policy and rule library are mutually satisfied, there should not be any variance in SAP GRC AC. The access control system provides all necessary information, from the rule library to the management report to the correct remediation process. In Figure 8.1, continuous compliance is defined in 3 phases: Get Clean, Stay Clean, and Stay in Control. Get Clean is the first step toward the compliance effectiveness and the capability of Risk Analysis and Remediation provides in-depth cleaning of access authorization in SAP and non-SAP systems.

![Continuous Compliance Diagram](image-url)

**Figure 8.1** Continuous Compliance
Simulation

Simulation is a proactive way to determine SoD violations before they happen. SAP GRC AC has the capability to perform simulations of user assignments, actions or permissions assignments, and role assignments. This functionality is not limited to SAP systems; SAP GRC AC can perform simulation analysis for cross systems and legacy systems.

As an example, consider a scenario where Basis Admin received a request from a user (BJONES) to add Transaction FD02 to his profile. You need to perform a simulation task for assigning this new action. Figure 8.2 shows the initial simulation screen.

Click on **Simulate** to display multiple options for actions that can be performed, such as Action, Role, or Permission (see Figure 8.3).
Note

If you are working with a role that has many transactions, we recommend running the simulation in background mode.

Figure 8.3 Simulation for User Level

In this example, the source systems for the risk analysis are an ERP system and a cross system. The report type can be defined for the action or permission level; in our example, we are processing for action only. The requestor has asked for Transaction FD02, in the SAP ERP system with the host name J1E. You can select Yes in the field Exclude Values in the above Figure 8.3, so that the output is limited to risks from the simulation selection criteria only.
In figure 8.4, the report output for simulation produces two action rule violations in the risk LR02. This simulation causes violations with risk LR02009 in the J1E system and with risk LR02004 in the legacy system.

When you have this information, you must decide on the transaction assignment to the user.

This example shows you how users can practice proactive compliance in SAP GRC AC.
8.3 Monitoring and Control

By regularly monitoring the activities of user access assignments and roles, you can improve the effectiveness of risk/control assessments. As previously discussed, SAP GRC AC provides alert monitoring to check critical transactions or conflicting violations, and also uses mitigation control to monitor SoD violations. Mitigation control can be effective for certain periods of time during the SoD cleanup process, and can also be used to support special projects.

In conclusion, the following are some of the main advantages of this functionality:

- Rapid identification of specific deficiencies through simulation and alert control.
- Reduction in errors and fraud by enforcing proactive compliance methodology.
- Reduction in costs thanks to a complete rule library.
- Documented evidence and audit trails for internal and external auditors.
- A management report for each calendar month and its progress violation count graphs.
- 25% cost reduction as a result of the automation of certain parts of the Sarbanes-Oxley (SOX) process such as enhancing repeatability and sustainability (statistic from a December 2005 AMR research study).
- According to a 2006 IIA survey, 38% of internal auditors say they plan to implement continuous monitoring in the future.

8.4 Summary

In this chapter, we covered the continuous compliance processes and the capability of Get Clean in the Risk Analysis and Remediation application. You learned about the simulation process and how the simulation is helpful in cross-system applications. By proper monitoring and control, you can improve the effectiveness of the compliance initiatives in your organization.
Index

A
Access Control, 9, 13
Actions, 71
Active Rules, 37
Alert dashboard, 103
Alert Monitor, 103
Analysis Engine Daemon Manager, 90
Asynchronous, 98
Asynchronous mode, 67

B
Background, 76
Background Job, 73, 81, 82

C
Cleared Alerts, 105
Comparison utility, 66, 75
Compliance Calibrator, 11, 21
Connector Creation, 59, 63, 64
Continuous compliance, 107
Create rules, 35
Cross-enterprise, 18
Cross-Enterprise Rules, 43
Cross-system IDs, 87
Cross-system risk analysis, 92

D
Data Extraction, 51, 70
Data Extractor, 65
DGN Technologies, 57

E
Enable, 38
Export, 50

F
Foreground, 76
Full mode, 81

G
Generate Rules, 24
Get Clean, 108
GRC triangle, 17
Greenlight, 58

I
Identity Management, 15
import, 50
Incremental mode, 81

J
JCO, 13
JCO Connector, 15
JDBC, 15, 59
JDBC Connector, 15
JDE, 63

L
Legacy Systems, 24, 64

M
Management reports, 85
Mitigation, 95
Mitigation controls, 95–96
Monitor, 96
Implementing SAP GRC

The book will provide implementation teams with a roadmap for using the pre-delivered configurations and mature features and functions of GTS as the basis for a rapid installation. At the same time, it covers the best practices necessary for setting the components up properly so that expansion, customization, and upgrading can be done easily downstream. The book is organized into short, focused, modular chapters that give the reader the hands-on planning and configuration guidance necessary for implementing either all of the GTS component, or only those pieces relevant to the organization's needs.

approx. 130 pp., 68,– Euro / US$ 85


www.sap-press.com

Index

N

NetWeaver, 13

O

Oracle, 59

P

PeopleSoft, 63
Permissions, 72
Profile, 69
Profile Action, 70

R

RAR, 10, 21
Real Time Agent, 13, 55, 57
Real time risk analysis, 86
Risk, 25, 35, 48
Risk analysis, 81
Risk Analysis and Remediation, 10, 21
Risk Identification, 48
Risk recognition, 48
Role, 69
Role Action, 69
RTA, 13, 55, 57
RTA Deployment, 64
Rule Architect, 21
Rule files, 54
Rule Library, 12, 47
Rule Migration, 48
Rules, 23
Rule sets, 23
Rule Transport, 49
Rule Wizard, 49

S

SAP GRC, 9
SAP JCO, 15
Sarbanes-Oxley, 9
Sarbanes-Oxley Act, 15
Scheduling, 84
Segregation of Duties, 9, 21
Simulation, 109
SLD, 14
SoD, 9, 10, 16, 21, 23, 47
SoD analysis, 107
SoD violations, 101
SoD violations, 95
SOX, 9, 15, 17
synchronization job, 82
System Connector, 67
System Landscape Directory, 14

U

UME, 14
unmitigated risks, 101
Uploading Rule Files, 25
Upload Objects, 26
User, 69
User Action, 69
User Management Engine, 14
User Mapping, 79
Utilities, 51

V

VIRSAHR, 57
VIRSANH, 57

W

WebDynpro, 22