This excerpt highlights how a properly implemented risk management solution can help you keep pace with risk. Learn how to automate and coordinate risk management activities and enable your business users to make better decisions and improve performance.

In Chapter 15, we cover the implementation process of SAP Risk Management and show you how effective a properly implemented solution can be.
SAP Risk Management helps organizations automate and coordinate risk management activities. Reliable and accurate risk information enables business users to make better decisions and improve performance. In this chapter, we cover the implementation process and show how customers realize business value from the solution.

15 SAP Risk Management Implementation

The number and diversity of risks grows as the business landscape become more complex, as companies expand and introduce new products, and as supply chains become more distributed. Often the capability of a business to manage these risks doesn’t keep pace. To understand and manage risks, businesses must understand the risk drivers, recognize how risks impact business value, anticipate catastrophic losses, mitigate risks, and act on emerging opportunities.

The SAP Risk Management solution automates the Enterprise Risk Management (ERM) process for an organization. In addition, financial institutions can enable additional solution functionality to support their Operational Risk Management (ORM) process. In this chapter, we’ll first look at an overview of Enterprise Risk Management (ERM) in Section 15.1 and then review the scenario in further detail, including business blueprints for implementation and system configuration in Section 15.2. Next we’ll turn our focus to the ORM scenario with an overview in Section 15.3 followed by similar details for implementation in Section 15.4.
15.1 Enterprise Risk Management Overview

Most customers when asked about their risk management practice generally talk about a lack of transparency and unavailability of accurate risk information for decision making.

Risk management teams are in a difficult situation. They are responsible for the risk management processes but typically don’t own the key risks—they are owned by the lines of business (LOBs). So they constantly struggle with follow-ups, progress, and tracking status of risks. They are also constantly wondering about risks that can blindside the organization.

Business owners and LOB managers typically aren’t thinking about risks per se but only about performance. They typically get several surveys or assessments from different groups that ask similar questions (not only from the enterprise risk group but also from audit, it security, business continuity, etc.). But because risk and performance are really just two sides of the same coin, they typically come up with good solutions to address the risks they know about—but only the risks they know about—and they have absolutely no visibility into risks outside of their silo that could negatively affect them. The risk mitigation efforts that are successful are one-offs and typically never reapplied to other regions or similar business units.

Executives are mainly concerned with market expectations and delivering on strategy, and they think about risks only as an afterthought. After the strategy is developed and plans are executed, they start to ask about risks. The result is that executives are left not knowing whether any negative surprises will keep them from meeting their business objectives until it’s too late.

SAP Risk Management enables the ERM process for an organization and in turn helps risk managers, business owners, and executives preserve and grow value by doing the following:

- Aligning risk management with business value drivers
- Creating continuous insight into the status of risk
- Acting on emerging risks and opportunities

Figure 15.1 shows the ERM process supported by the SAP Risk Management solution. Figure 15.1 describes the solution capabilities and closely aligns with best practice ERM frameworks such as ISO 31000 and COSO II ERM.

Figure 15.1 The Five Components of Enterprise Risk Management

Let’s look at each of these five components shown in Figure 15.1 in a little bit more detail as it relates to ERM:

- **Plan**
  ERM begins with planning. Planning enables organizations to focus risk management implementation on what is most relevant for their business. Planning ensures that the risk management initiative starts with a complete understanding of context, business value drivers, risk appetite, threshold levels, and business objectives to be achieved.

- **Link**
  The link component is the next phase. Risks are identified, documented, and aligned with the business context—drivers/causes, impacts/consequences, organizations, risk categories, activities, and objectives.
Next, risks are analyzed using quantitative and qualitative methods for prioritization and developing effective treatment strategies.

Risk evaluation helps select the risks (and opportunities) for treatment by balancing the costs of implementing each option against the benefits derived from it.

This component covers monitoring of the effectiveness and completeness of the risk treatments, taking corrective actions, and communicating the status of risks.

Now that we have a conceptual understanding of ERM, let's explore this in further detail.

**15.2 Enterprise Risk Management Scenario**

The maturity of ERM practices typically varies across customers. Hence, prior to delving into the implementation process, let's review a customer adoption model. SAP Risk Management has many features and functionalities, but not all may be applicable for a particular customer. In fact, customers might prefer to adopt the solution functionality in multiple phases based on their level of risk management maturity.

Tables 15.1 through 15.3 show a three-part solution adoption model for customers. The model aligns customer requirements with solution functionality on an increasing level of risk management maturity and expectation of business benefits. The three-part model can also be thought of as a three-phase solution implementation approach. Breaking out the implementation into multiple phases helps faster realization of business value for the customer. Note that this model is simply a recommendation, and customers can choose to ignore it and/or use a hybrid approach.

Table 15.1 describes the minimal solution adoption for customers. The goal in this phase is process automation that will help streamline risk management efforts across the organization and reduce costs.

Next, customers can leverage additional solution functionality for proactive risk prevention, as described in Table 15.2.

Customers with highly mature risk management practices can leverage risk information for decision making and to improve performance, as described in Table 15.3.
Now that we've explored the customer adoption model, let's shift our focus to the solution implementation process. The ERM scenario is the standard implementation scenario for SAP Risk Management. A typical solution implementation project is described in Figure 15.2. The project follows the traditional SAP implementation process of project preparation, business blueprint, realization, final/preparations, and then go-live. Completion of each major phase of the project is marked with a milestone.


The business blueprint stage is the most critical phase of an implementation project. The business blueprint captures customers’ requirements, project scope, and details on how to set the SAP Risk Management solution. The other stages in the project—preparation, realization, final preparations, and go-live—are standard for implementing any GRC solution and don’t necessarily capture details specific to SAP Risk Management. Hence, in this chapter, we’ll focus on the process of generating a business blueprint for the ERM scenario. We’ll review key activities and business challenges for the blueprint stage of the implementation project.

15.2.1 Business Blueprint

The objective of this most critical phase of the project is to understand the customer’s ERM process and business requirements. The business blueprint document captures the customer’s business requirements, mapping the requirements to solution functionality, along with details about system configuration and data setup. The business blueprint is developed in close consultation with the business users and serves as a reference scope document for the solution implementation.

Typically, the customer’s IT department proceeds in parallel to procure the servers (DEV/QAS/PRD) and install SAP NetWeaver Application Server ABAP (AS ABAP).

Next, we describe how to complete the several blueprinting tasks before launching into the realization phase of the ERM implementation. In the following sections, we’ll review:

- Solution configuration
- Data conversion
- Authorizations
- Workflows
- Reporting

15.2.2 Solution Configuration

In the solution configuration task, the customer business requirements are mapped to the SAP Risk Management Customizing Implementation Guide (Transaction SPRO). The parent Governance, Risk, and Compliance node in the IMG specifies customizing entries for all GRC solutions. The IMG entries listed in Figure 15.3 are required to be setup for...
the SAP Risk Management solution. Documentation for each IMG entry is available as part of Transaction SPRO.

Start with the Risk and Opportunity Attributes IMG entries under the Shared Master Data Settings node as shown in Figure 15.3. This configuration specifies the drivers, impacts, and benefits categories.

Next you set up the IMG entries along with all of the subentries, which are available under the Common Component Settings node as shown in Figure 15.4. The IMG entries under the Common Component Settings are applicable across all GRC solutions and need to be set up even when only implementing SAP Risk Management. Set up the following entries:

- **Integration Framework**
  Set up connectors for the SAP NetWeaver Portal, email, Active Directory, SAP HANA database, web services, and other data sources.

- **Policy Management**
  Set up the common component of SAP Policy Management.

- **Ad Hoc Issues**
  Set up the common component of Issue Management.

- **Planning and Scheduling**
  Set up the SAP Risk Management planner activities. Planner is the common SAP GRC planning and scheduling tool. These activities are described in further detail in the “Workflows” section later in this chapter.

Finally, set up all of the IMG entries and subentries under the Risk Management node as shown in Figure 15.5. This node captures SAP Risk Management specific system configuration. Set up the following:

- **General Settings**
  Set up change history and risk terminology.

- **Master Data Setup**
  Set up types, categories, units of measure, and other attributes of the SAP Risk Management master data entities.

- **Risk and Opportunity Analysis**
  Set up configuration for risk analysis and risk heatmaps (risk impact and risk probability matrix).

- **Response and Enhancement Plan**
  Set up configuration for the different types of risk responses: mitigations, controls (integration with SAP Process Control), policies, and issues.

- **Incident and Loss Database**
  Set up configuration for the incident and loss database in SAP Risk Management.

- **Key Risk Indicators**
  Set up configuration for the KRIs, including connectors, data sources, and KRI classification.
15.2.3 Data Conversion and Master Data Setup

In the data conversion task, customer business requirements are mapped to the SAP Risk Management master data elements. Requirements are documented to set up the following master data objects available under the Master Data work center as shown in Figure 15.6:

- **Business Objectives**
  - A two-level taxonomy that defines risk strategies and objectives.

- **Organizations**
  - An N-level taxonomic structure that defines the risk management organization structure. Organizations also capture additional attributes such as applicable business objectives, units of measure, risk appetite, risk threshold/impact levels, roles with user assignments, and any other additional information.

- **Policies**
  - Policy categorization along with risk management policies in use.

- **Activity Hierarchy**
  - Multiple N-level taxonomic structures that define business activities for risk management. One or more taxonomic structures can be set up to capture the additional dimensions for risk management such as business processes, projects, products/services, and so on.

- **Risk Catalog**
  - An N-level taxonomic structure that defines risk category structure along with risk templates.
The first level defines the strategy and is simply a classification element. The second level defines the objective, which will be aligned with organizations. Objectives can also be categorized as shown in Figure 15.8 with the list of categories being defined in the IMG customizing.

Organizations

Organization structure is the central common master data entity in SAP GRC. The organization structure is a shared entity among SAP Risk Management, SAP Process Control, and SAP Access Control. The majority of SAP GRC workflows are routed based on the organization role settings.

Organizations can be accessed using the ORGANIZATIONS quick link in the ORGANIZATIONS section on the MASTER DATA work center as shown earlier in Figure 15.6. An organization is an N-level taxonomic structure that defines the SAP GRC organization structure as shown in Figure 15.9.

Figure 15.10 shows the details for an organizational element. Because the organizations structure is a shared master data entity, it contains a lot of settings and tabs, not all of which are applicable for the ERM setup as shown in Figure 15.10.
Table 15.4 describes details of the setup necessary for the various tabs for an organizational element.

<table>
<thead>
<tr>
<th>Organization Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GENERAL</strong></td>
<td>Capture general attributes for an organization. Only the <strong>NAME</strong>, <strong>DESCRIPTION</strong>, <strong>VALID TO</strong>, and <strong>CURRENCY</strong> attributes are mandatory for ERM. The <strong>VALID TO</strong> attribute is used to define the validity time frame for an organization. As organization structures frequently change, this attribute is useful to retire older organizations and hide the related information from SAP Risk Management.</td>
</tr>
<tr>
<td><strong>POLICIES</strong></td>
<td>Show the list of policies and procedures applicable for the organization. The use of this tab is optional for ERM. SAP Policy Management is a common SAP GRC component for managing policies and procedures.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OBJECTIVES</strong></td>
<td>Select objectives from the BUSINESS OBJECTIVES hierarchy and link with the organization. This linkage narrows the list of objectives available for a risk that is part of the organization.</td>
</tr>
<tr>
<td><strong>RISK SUMMARY</strong></td>
<td>Show an aggregated risk level and assessment summary for all risks defined for the organization. As users use the system, document, and analyze risks, details shown on this tab are updated.</td>
</tr>
<tr>
<td><strong>UNITS OF MEASURE</strong></td>
<td>Define a unit of measure setting for each risk impact category that will convert risk analysis for the impact into a monetary amount based on the applicable currency. This setting is mandatory when using the quantitative risk analysis profile.</td>
</tr>
<tr>
<td><strong>RISK APPETITE</strong></td>
<td>Define the risk appetite for the organization in quantitative and qualitative measures. This setting is mandatory for risk analysis.</td>
</tr>
<tr>
<td><strong>RISK THRESHOLDS</strong></td>
<td>Define the quantitative lower and upper limits for each of the risk impact levels. This setting is mandatory for risk analysis.</td>
</tr>
<tr>
<td><strong>ROLES</strong></td>
<td>Define the user assignments for the entity-role combinations for an organization. This process is described in the “Authorization Concept and Roles” section later in this chapter. From the available list of roles on this tab, only the following roles need to be defined for ERM: CEO/CFO, CENTRAL RISK MANAGER, INCIDENT EDITOR, INTERNAL AUDITOR, ORGANIZATION OWNER, SYSTEM ADMINISTRATOR, and UNIT RISK MANAGER.</td>
</tr>
<tr>
<td><strong>ISSUES</strong></td>
<td>Create and view ad hoc issues for the organization. The use of this tab is optional for ERM. Issue Management is another common SAP GRC component for logging and remediation of SAP GRC issues.</td>
</tr>
<tr>
<td><strong>ATTACHMENTS AND LINKS</strong></td>
<td>Define additional information for an organization by either attaching documents or specifying URL links. The use of this tab is optional for ERM.</td>
</tr>
</tbody>
</table>

**Figure 15.10** Organization Definition

Table 15.4 Organization Settings

Configuration and details for tabs for an organizational element
Policies
SAP Policy Management is a common SAP GRC component for managing policies and procedures. Policies can be accessed using the POLICIES quick link in the REGULATIONS AND POLICIES section on the MASTER DATA work center as shown in Figure 15.6. SAP Policy Management is covered in Chapter 9 earlier and hence not described in detail here. Use of policies and procedures is optional for ERM. Customers that use policies and procedures can align risks with policies and also use procedures as risk treatment measures.

Activity Hierarchy
Enterprise risks are generally aligned with business activities. Business activities can represent any taxonomic structures such as business processes, projects/programs, products/services, assets, and so on. Use of activity hierarchy is optional for ERM, and customers that need to do so will need to use this master data entity. When using the ACTIVITY HIERARCHY, additional transaction data defined as ACTIVITIES also need to be defined prior to aligning risks with activities. The ACTIVITIES transactional element is described later in this section and assigns the ACTIVITY HIERARCHY with an organization and user-role combination.

The activity hierarchy can be accessed using the ACTIVITY HIERARCHY quick link in the ACTIVITIES AND PROCESSES section on the MASTER DATA work center as shown earlier in Figure 15.6. ACTIVITY HIERARCHY consists of multiple N-level taxonomic structures that define business activities for risk management as shown in Figure 15.11.

The SHOW dropdown shown in Figure 15.11 defines multiple taxonomic structures for different activity types. The activity types shown here are defined in IMG customizing. Note that only a single such structure is usually necessary for a customer. A single risk can only be aligned with one business activity. However, different types of risks may use different types of activities and hence, multiple structures are supported. Figure 15.12 shows the definition for an activity hierarchy element.

Table 15.5 describes details of the setup necessary for the various tabs for an activity hierarchy.
The risk catalog can be accessed using the Risk Catalog quick link in the Risks and Responses section on the Master Data work center as shown earlier in Figure 15.6. The Risk Catalog is an N-level taxonomic structure that defines the risk category structure along with risk templates as shown in Figure 15.13. A risk classification structure is mandatory for ERM. Use of risk templates is optional, however.

### Activity Hierarchy Tab

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GENERAL</strong></td>
<td>Capture general attributes for an activity hierarchy such as NAME, DESCRIPTION, and VALID TO. The VALID TO attribute is used to define the validity time frame for an activity hierarchy. The ALLOW ACTIVITY ASSIGNMENT attribute defines whether activities can be defined for the particular activity hierarchy element.</td>
</tr>
<tr>
<td><strong>GENERAL (Cont.)</strong></td>
<td>Because these are in a taxonomic structure, activities may not be applicable for parent (or top-level) nodes, and such configuration can be controlled with this attribute.</td>
</tr>
<tr>
<td><strong>RISK CLASSIFICATION</strong></td>
<td>Certain activity hierarchy elements may only be applicable for certain risk categories. This kind of filtering is optional but when necessary can be defined using the Risk Classification tab.</td>
</tr>
<tr>
<td><strong>OPPORTUNITY CLASSIFICATION</strong></td>
<td>Certain activity hierarchy elements may only be applicable for certain opportunity categories. This kind of filtering is optional but when necessary can be defined using the Opportunity Classification tab.</td>
</tr>
<tr>
<td><strong>ATTACHMENTS AND LINKS</strong></td>
<td>Define additional information for the activity hierarchy by either attaching documents or specifying URL links. The use of this tab is optional for ERM.</td>
</tr>
</tbody>
</table>

Table 15.5 Activity Hierarchy Settings

### Risk Catalog

The different nodes of the risk catalog define the risk categorization structure for ERM. Details of one such risk category is shown in Figure 15.14.
Table 15.6 describes details of the setup necessary for the various tabs for a risk category.

<table>
<thead>
<tr>
<th>Risk Category Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Capture general attributes for a risk category such as NAME, DESCRIPTION, and VALID TO:</td>
</tr>
<tr>
<td></td>
<td>The VALID TO attribute is used to define the validity time frame for a risk category.</td>
</tr>
<tr>
<td></td>
<td>The ALLOW ACTIVITY ASSIGNMENT attribute defines whether risks can be defined for the particular risk category element. Because these are in a taxonomic structure, risks may not be applicable for parent (top-level) nodes, and such configuration can be controlled with this attribute.</td>
</tr>
<tr>
<td></td>
<td>The ANALYSIS PROFILE attribute defines the applicable risk analysis profile for risks belonging to risk category. The risk analysis profile is set up in IMG customizing and defines the method of risk assessment. Different types of risk assessment configurations are possible and made applicable for different risk types using this attribute. To keep things simple, customers typically use a single analysis profile to assess all enterprise risks. In such a case, a single value is available for selection in this attribute. A single risk profile for managing all enterprise risks is also recommended to make risk aggregation, consolidation, and comparison easier.</td>
</tr>
<tr>
<td></td>
<td>The IS SECONDARY TOP NODE attribute is only applicable for the ORM scenario and is described later in this chapter.</td>
</tr>
<tr>
<td></td>
<td>The LEADING FORECASTING HORIZON attribute is used when risk assessment needs to be performed for one or more time frames (forecasting horizons). This type of risk assessment is only applicable for CORPORATE risk types and isn’t covered in this chapter. Refer to SAP Note 1649904 (<a href="https://service.sap.com/support/notes/1649904">https://service.sap.com/support/notes/1649904</a>) for more details on corporate risks.</td>
</tr>
</tbody>
</table>

Table 15.6  Risk Category Settings (Cont.)

Risk templates can be used to capture common risk definitions that include drivers, impacts, response templates, and central controls. A company might have multiple business units, and certain risks (such as IT risks or supply chain risks) can be common for all of the business units. Customers might want to capture a common definition of such a risk as a template and then distribute (create instances) the template for each business unit. Each such risk instance will have the basic structure of the risk template but can be further localized by risk owners and risk assessment applicable for the particular business unit. Distribution of risk templates is possible using two methods—copy and reference. Risk templates distributed with the copy method allow local risk owners to change the risk definition obtained from the template. Risk templates distributed with the reference method don’t allow local risk owners to change the risk definition obtained from the template. Additional risk details that aren’t obtained from the template, along with risk assessments, can always be changed for all risks.

Use of risk templates is optional and when required can be defined for any risk category. Risk templates appear as leaf nodes in the risk catalog structure. Details of one such risk template is shown in Figure 15.15.
Configuration and tab details for the setup of a Risk template

Table 15.7 describes details of the setup necessary for the various tabs for a risk template.

### Risk Template Tab Description

<table>
<thead>
<tr>
<th><strong>GENERAL</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Capture general attributes for a risk category such as NAME, DESCRIPTION, RISK TYPE, and VALID TO. The VALID TO attribute is used to define the validity time frame of a risk template.</td>
<td></td>
</tr>
<tr>
<td>- The RISK TYPE attribute can either be set as OPERATIONAL or CORPORATE. Operational risks have multiple impacts and single time frame-based assessments. This is the default risk type referred to in this chapter for both ERM and ORM scenarios.</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 15.15** Risk Template Definition

Table 15.7  Risk Template Settings (Cont.)

**Response Catalog**

The response catalog can be accessed using the RESPONSE CATALOG quick link in the RISKS and RESPONSES section on the MASTER DATA work center as shown earlier in Figure 15.6. The response catalog is a flat structure that captures response templates as shown in Figure 15.16.

Use of the response catalog is optional for ERM. Details of one such response template are shown in Figure 15.17.

Table 15.8 describes details of the setup necessary for the various tabs for a response template.

**Table 15.7** Risk Template Settings (Cont.)

<table>
<thead>
<tr>
<th>Risk Template Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RISK INSTANCES</td>
<td>Lists the instances of (local) risks that are created using this risk template.</td>
</tr>
<tr>
<td>RESPONSE TEMPLATES</td>
<td>Define the response templates associated with the risk template.</td>
</tr>
<tr>
<td>CENTRAL CONTROLS</td>
<td>Define the central controls associated with the risk template.</td>
</tr>
<tr>
<td>ATTACHMENTS AND LINKS</td>
<td>Define additional information for the risk template by either attaching documents or specifying URL links. The use of this tab is optional for ERM.</td>
</tr>
</tbody>
</table>
Configuration and tab details for the setup of a response template

<table>
<thead>
<tr>
<th>Response Catalog Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Capture general attributes for a response template such as Name, Description, and Valid To:</td>
</tr>
<tr>
<td></td>
<td>▶ The Valid To attribute is used to define the validity time frame for a response template.</td>
</tr>
</tbody>
</table>

**Figure 15.16** Response Catalog Structure

**Figure 15.17** Response Template Definition

**Table 15.8** Response Template Settings (Cont.)

**KRI Templates**

The final master data entity is the KRI templates entity that can be accessed using the KRI Templates quick link in the Key Risk Indicators section on the Rule Setup work center as shown in Figure 15.18.

KRI templates capture categorization and classification for KRIs that are used in ERM. Hence, KRI templates need not be set up if KRIs aren’t being used. Figure 15.19 shows a sample list of KRI templates.
Details of one such KRI template is shown in Figure 15.20.

Table 15.9 describes details of the setup necessary for the various tabs for a KRI template.

- **General**
  - Capture general attributes for a KRI template such as **NAME**, **DESCRIPTION**, **VALID TO**, and others:
    - The **VALID TO** attribute is used to define the validity time frame for a KRI template.
    - The **VALUE TYPE** attribute specifies the type of KRIs (NUMBER, CURRENCY, QUANTITY, SCORE, etc.) applicable for this template. The selections available for these attributes are defined in IMG customizing.
    - The **RISK CATEGORY** is a read-only attribute that shows the risk category linked with the KRI template.
    - The **SYSTEM**, **BUSINESS PROCESS**, and **COMPONENT** attributes are optional and capture a three-level classification structure for KRI templates. The selections available for these attributes are defined in IMG customizing.
The Master Data Upload Generator (MDUG) tool is currently only available for SAP Process Control. However, as the organizations, policies, and risk catalog entities are shared between SAP Process Control and SAP Risk Management, MDUG can be used to upload them. The remaining entities (business objectives, activity hierarchy, response catalog, and KRI templates) described previously have to be set up manually in SAP Risk Management.

Often customers manage risks using spreadsheets and other documents prior to leveraging SAP Risk Management. Hence, in addition to the master data entities described earlier, customers often have lists of activities, risks, and incidents they want to load into the solution. SAP Risk Management supports upload for such transactional data for activities, risks, and incidents. If such information needs to be set up in the SAP Risk Management system, capture the details in the blueprint document, and use the following process and screens shown to set up this data.

To upload these transactional data entities, first go to the Assessments work center as shown in Figure 15.21.

Activities

Use the ACTIVITIES quick link under the RISK ASSESSMENTS section to upload activities. This shows the list of ACTIVITIES in the system. Use the UPLOAD menu button available on this screen (see Figure 15.22) to upload activities from a Microsoft Excel or XML document. Use the DOWNLOAD menu button to generate the upload file format document.

Risks

Use the RISKS AND OPPORTUNITIES quick link under the RISK ASSESSMENTS section to upload risks. This shows the list of RISKS in the system. Use the UPLOAD menu button available on this screen as shown in Figure 15.23.
15.23 to upload risks from a Microsoft Excel or XML document. Use the Download menu button to generate the upload file format document.

**Figure 15.23** Upload for Risks

Incidents

Use the Incident Management quick link under the Incident Management section to upload incidents. This shows the list of Incidents in the system. Use the Upload menu button available on this screen as shown in Figure 15.24 to upload incidents from a Microsoft Excel or XML type document. Use the Download menu button to generate the upload file format document.

**Figure 15.24** Upload for Incidents

Customers may also use surveys and questionnaires for risk assessments. If these also need to be set up in the system, capture the details in the blueprint document. Use the quick links in the Surveys section in the Assessments work center as shown earlier in Figure 15.21 to set up this data.

15.2.4 Authorization Concept and Roles

The SAP Risk Management application is based on the SAP NetWeaver authorization model and assigns authorizations to users based on roles. SAP standard roles (Transaction PFCG basic roles) provide the technical standard authorizations to the ABAP server. These roles are hierarchical and provide top-down authorizations. Roles at a higher entity level have greater authorizations to perform tasks and greater access to the application than roles at a lower entity level. This hierarchy also affects task assignments, workflows, and business event processing. Furthermore, a second-level authorization allows restriction of the user selection for entity-level role assignments. So only those users who have been assigned the corresponding Transaction PFCG role in their user profile are available for an assignment.

To use SAP Risk Management, the following three types of roles must be set up and activated.

- **SAP NetWeaver Portal role**
  This role enables users to configure the portal navigation structures and menu tabs. This role should be assigned to all SAP Risk Management users either directly or via a group in the portal. The administrator must ensure that the portal interface can be accessed with the correct level of authorization by all other users.

- **Standard or backend roles**
  These roles define the authorizations in the backend system, where, for example, customizing is done. This kind of role should be assigned to users that require a backend user profile. The standard roles that are delivered with the SAP Risk Management application are the following:

  - **Basic role (SAP_GRC_FN_BASE)**: The basic technical role for a user who wants to use SAP Risk Management. This role contains all necessary authorizations to make the necessary customizing settings for this application. This role doesn’t contain any authorizations for the portal interface.

  - **Business user (SAP_GRC_FN_BUSINESS_USER)**: A user with this role is only authorized to perform operations on assigned entities in SAP Risk Management. It’s recommended that a user with this role also be assigned a portal role for SAP Risk Management to use the web interface of the application.

  - **Power user (SAP_GRC_FN_ALL)**: In addition to the authorizations of the business user, a power user also has authorization for administrative functions in customizing, such as the definition of organizational units.
Display user (SAP_GRC_FN_DISPLAY): A user with this role can display all risk data in the portal. This role is useful for external auditors.

The portal administrator can use these standard roles directly. Administrators can also copy the delivered roles, makes any necessary adjustments to suit customer needs, and assign the modified copy of the standard roles to the end users to grant them the required access to the SAP Risk Management application. Administrators can copy and adjust these default roles in customizing (Transaction PFCG).

Application roles
These roles refine the authorizations delivered in the business user standard role (SAP_GRC_FN_BUSINESS_USER) to support application-specific operations such as create, edit, and delete for different application entities such as organizations, risks, and activities.

SAP Risk Management includes additional application roles, as detailed in Table 15.10.

<table>
<thead>
<tr>
<th>Application Role Name</th>
<th>Business Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_GRC_RM_API_ACTIVITY_OWNER</td>
<td>Activity owner</td>
</tr>
<tr>
<td>SAP_GRC_RM_API_CENTRAL_Risk</td>
<td>Central risk manager</td>
</tr>
<tr>
<td>SAP_GRC_RM_API_CEO_CFO</td>
<td>CEO/CFO</td>
</tr>
<tr>
<td>SAP_GRC_RM_API_INCIDENTEDITOR</td>
<td>Incident editor</td>
</tr>
<tr>
<td>SAP_GRC_RM_API_INTERNAL_AUD</td>
<td>Internal auditor</td>
</tr>
<tr>
<td>SAP_GRC_RM_API_LIAISON</td>
<td>System administrator</td>
</tr>
<tr>
<td>SAP_GRC_RM_API_OPP_OWNER</td>
<td>Opportunity owner</td>
</tr>
<tr>
<td>SAP_GRC_RM_API_ORG_OWNER</td>
<td>Organization owner</td>
</tr>
<tr>
<td>SAP_GRC_RM_API_RISK_MANAGER</td>
<td>Unit risk manager</td>
</tr>
<tr>
<td>SAP_GRC_RM_API_RISK_OWNER</td>
<td>Risk owner</td>
</tr>
<tr>
<td>SAP_GRC_RM_API_RISK_EXPERT</td>
<td>Risk expert</td>
</tr>
</tbody>
</table>

Table 15.10 SAP Risk Management Application Roles

Application roles are also maintained and modified using Transaction PFCG. SAP GRC customizing (Transaction SPRO) is used to assign application roles to entities such as organizations, activities, opportunities, risks, and incidents. Users are finally assigned to the entity-role combination in the SAP Risk Management application frontend. Single or multiple users can be configured for assignment to each entity-role combination. The following three-step process is shown in Figure 15.25:

Use the standard application roles available with SAP Risk Management, or copy the role and make updates. This can be accomplished using Transaction PFCG.

Assign roles to GRC entities, such as org. units
Assign users to roles assigned to entities
Assign users to the entity-role combination. This is accomplished in the frontend portal. Each entity, such as organizations, activities, risks, and incidents, can be assigned.
incidents, has a ROLES tab. Using this tab, one or more users, depending on the configuration in the preceding step 2, can be assigned to the entity-role combination.

In this part of the blueprinting exercise, users, roles, role modifications, entity-role assignments, and user to entity-role assignments are identified and documented.

15.2.5 Workflows
SAP Risk Management ships with a set of workflows that enable collaboration on risk management activities within a company by making use of the standard SAP workflow functionality. SAP workflows are based on the guided procedures that walk users through a risk management activity or process. Workflow examples include collaborative risk reassessments, validation of assessment results, or reviews of a newly documented risk. There are two types of workflows in SAP Risk Management: event-based workflows and planner-based workflows.

Event-Based Workflows
Event-based workflows are predefined end-to-end processes triggered by user actions such as proposing a risk or KRI alerts. Event-based workflows are defined using business events: A business event involves the assignment of a workflow task to a recipient, which is also known as agent determination.

Agent determination is the system process that assigns users to workflows. The entity-based authorization concept in SAP Risk Management is used for agent determination in workflow processing. For each usage of agent determination, a business event is determined. A business event is a placeholder for recipient determination in workflow-driven scenarios or surveys, and the workflow processor or survey recipient is considered the agent. For agent determination, the implementation team maps the SAP Risk Management roles to the business events in customizing (Transaction SPRO). The assignment of business events to SAP Risk Management application roles in customizing is optional. If no customizing has been defined here, the workflows route to the users defined under the ROLES tab for the relevant entity. This default system behavior might be suitable for most customers. When the workflow or survey requires the agent, it triggers the agent determination rule with the corresponding business event and object ID.

Table 15.11 details the event-based workflows that are found in SAP Risk Management.

<table>
<thead>
<tr>
<th>Workflow Name</th>
<th>Description</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propose Risk</td>
<td>Ensures that users review a (potential) risk entered through the PROPOSE Risk function and rework it if necessary before adding it to the risk database.</td>
<td>User entry through MY HOME • AD HOC TASKS • RISK PROPOSAL</td>
</tr>
<tr>
<td>Report Incident</td>
<td>Ensures that users check a reported incident for completeness and accuracy before adding it to the incident database.</td>
<td>User entry through MY HOME • AD HOC TASKS • INCIDENTS</td>
</tr>
<tr>
<td>KRI Implementation Request</td>
<td>Ensures the proper configuration and system setup for KRI-related data, which should be available for risk monitoring.</td>
<td>KRI implementation request</td>
</tr>
<tr>
<td>KRI Localization Request</td>
<td>Optional adjustment of an assigned KRI with respect to risk-specific settings.</td>
<td>KRI localization request</td>
</tr>
<tr>
<td>Propose Control</td>
<td>Allows users (e.g., risk managers) to propose a control to mitigate a risk. The control becomes part of the regular monitoring activities in SAP Process Control.</td>
<td>PROPOSE • CONTROL button on the RESPONSE PLANS tab for a risk</td>
</tr>
</tbody>
</table>

Table 15.11 Risk Management Event-Based Workflows, Descriptions, and System Triggers

Now that we’ve looked at the event-based workflows and their triggers, let’s look at the planner-based workflows.

Planner-Based Workflows
Planner is the common scheduling and planning tool for all SAP GRC solutions. Planner can be accessed under the ASSESSMENTS work center.
on the SAP GRC portal. Planner-based workflows are planned and triggered through the SAP Risk Management Planner function, such as updating a risk or creating a risk survey. These workflows route to the appropriate recipients and appear as tasks in the users Work Inbox.

SAP Risk Management contains the planner-based workflows detailed in Table 15.12.

<table>
<thead>
<tr>
<th>Workflow Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Validation</td>
<td>Allows a planner (e.g., a risk manager) to obtain sign-off and confirmation for the current risk situation for an activity (such as a process, project, or company asset).</td>
</tr>
<tr>
<td>Risk Validation</td>
<td>Enables the risk manager to obtain sign-off and confirmation for the current risk (including the assigned responses).</td>
</tr>
<tr>
<td>Opportunity Validation</td>
<td>Enables the risk manager to obtain sign-off and confirmation for the current opportunity (including analysis and assigned enhancement plans).</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Supports risk managers to initiate risk assessments (simple assessments, collaborative assessments, and survey-based assessments).</td>
</tr>
<tr>
<td>Opportunity Assessment</td>
<td>Supports opportunity managers to initiate opportunity assessments.</td>
</tr>
<tr>
<td>Response Update</td>
<td>Enables risk managers and risk owners to keep track of current risk responses.</td>
</tr>
</tbody>
</table>

Table 15.12 Planner-Based Workflows in SAP Risk Management

The workflow customizing (Transaction SPRO) activities as outlined in Table 15.13, (under Governance, Risk and Compliance • General Settings • Workflow) must be carried out to enable SAP Risk Management workflows.

<table>
<thead>
<tr>
<th>Customizing Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain Custom Agent Determination Rules</td>
<td>Specifies the agent determination rules to be used for business events in SAP Risk Management</td>
</tr>
</tbody>
</table>

Table 15.13 Customizing Activities in SAP Risk Management (Cont.)

Now that we’ve covered workflows, let’s move on to reporting.

15.2.6 Reporting

As recommended when we discussed the customer adoption model, it’s best to start by using the standard reports and analytics available under the Reports and Analytics work center as shown in Figure 15.26.

ERM reports are available through the quick links under the Risks and Opportunities and the Incidents and Losses sections shown in Figure 15.26. The SAP Risk Management dashboards are available through the quick links under the Management section. The SAP Risk Management 10.0 Learning Maps on the SAP Service Marketplace provide details on all of the Reports and Analytics quick links shown in Figure 15.26.

However, often there is a need for custom reporting, and the requirements can be documented in the blueprint. SAP NetWeaver Business Warehouse, SAP Business Intelligence solutions, Operational Data Provider (ODP, SAP NetWeaver 7.40), and SAP HANA Live can be used for developing custom reports and analytics. SAP Risk Management includes reporting content to support all of these tools.

In Section 15.2.1, we outlined the process for generating a business blueprint document for the ERM scenario. The blueprint document is then used to configure the solution, set up master data, set up user authorizations, enable workflows, and develop custom reports if necessary. After this is complete, the implementation goes through user acceptance and integration testing. Modifications are made to the implementation based on the outcomes from the user acceptance testing. After users sign off on the readiness of system setup, the installation is replicated to the production environment use of ERM commences.
If there are subsequent phases in ERM implementation, or the customer advances to the next stage in the adoption model outlined in the beginning, the same process should be repeated.

Now that we’ve fully explored ERM—the standard implementation of SAP Risk Management—from project preparation all the way to go-live, let’s look at how customers in certain industries can additionally leverage the embedded Operational Risk Management functionality.

### 15.3 Operational Risk Management Overview

The SAP Risk Management license includes the Operational Risk Management (ORM) functionality applicable for financial institutions—banks, insurance, automotive companies with finance divisions, as well as energy and utility companies involved in commodities trading. The default solution installation has the ORM functionality turned off. Before we discuss how to enable this additional functionality, let’s define ORM, the need for financial institutions to manage operational risk along with enterprise risk, and the benefits such customers can expect from the solution.

More than ever, financial institutions are investing in IT solutions to automate and optimize GRC activities. Fraught with change, unpredictability, and risk, today’s business environment demands an effective ORM strategy.

Additionally, regulatory requirements such as the Basel II Capital Accord (Basel II), the planned Basel III Capital Accord (Basel III), and Solvency II require comprehensive measurement of both internal and external risks. An organization must focus simultaneously on in-house process controls for fraud detection, employment practices, and workplace safety, as well as understand the impact of external factors on the business and have failovers in place in case of IT system failures.

In addition to obtaining reports from various LOBs, organizations must create an enterprise view of risk that reflects and measures potential threats to the institution. With the entire organization exposed to operational risk, decisions and recommendations to management must satisfy both existing and upcoming regulations and standards as well as align with the enterprise strategy.

Traditional ORM methods, where bits of information are rolled up from various LOBs, are no longer sufficient to achieve these goals. To create real value through an ORM process, an organization must evaluate the exposure of the whole institution in line with its business strategy. While meeting these business challenges, one must also understand potential exposures of IT systems. Additionally, management and regulators expect financial institutions to integrate external risk factors into a holistic picture of the risks it faces.

ORM enables customers to do the following:

- Measure, monitor, and control through KRIIs.
- Improve profitability through more accurate and future-oriented risk measurement.
- Satisfy regulatory requirements such as Basel II, Basel III, and Solvency II.
- Integrate ORM processes with existing operational systems such as HR, credit processing, and transactional banking systems.
- Integrate ORM into enterprise risk reporting alongside credit risk, market, and liquidity risk management.
- Support loss and capital reduction.
- Increase rating agency confidence and profitability.
- Optimize risk mitigation through integration with the SAP Access Control application and the SAP Process Control solutions.

Customers that want to use the ORM functionality can use SAP Note 1601962 (https://service.sap.com/support/notes/1601962) to turn on the following additional features:

- Static data management
  Managing multidimensional interlinked structures to support organizational-, process-, and product-dependent views over time.

- Loss event management
  Categorizing and distributing losses with capital allocation embedded in flexible workflows, and grouping losses and mitigating risks to protect against recurrence of loss.

- KRIs
  Integrating with operative systems to automate the data collection and updating process for KRIs, and supporting calculation rules for highly flexible dynamic aggregation.

- Risk control self-assessment
  Creating surveys that include dynamic result aggregation, and assessment workshop with a graphical user interface that provides complete access to the data repository.

- Scenario analysis and risk engine
  Enabling scenario analysis through risk analysis combined with scenario loss generation, and supporting approaches for Basel II (basic indicator approach [BIA], standard approach [STA], and advanced measurement approach [AMA]) and Basel III (grouped losses).

- Quantitative requirements
  Obtaining high-quality calibration results based on various distributions and supporting the most prominent loss distribution approach with Monte Carlo simulations with the SAP NetWeaver certified solution OpVision (www.opvision.es) from SAP Partner Quantitative Risk Research (QRR, www.qrr.es).

- Reporting
  Enabling system-specific and enterprise-wide reporting that includes comprehensive analytical interactive reports and dashboards customizable for different management levels.

- SAP Access Control and SAP Process Control
  Enabling deeper risk mitigation through integration with SAP Access Control (access risk and SoD management) and SAP Process Control (internal control management).

Similar to our approach in the ERM sections, we’ll explore an ORM implementation scenario and follow the implementation process from business blueprinting to go-live.

15.4 Operational Risk Management Scenario

Financial institutions need to manage operational risk to meet certain external regulatory requirements as well as internal requirements. Typically, the approach and functionality used for ORM varies based on the size of the institution. Hence, similar to our approach in Section 15.2, prior to delving into the implementation process, let’s review a customer adoption model.

Note
Prior to using the specific ORM functionality, customers have to implement the standard ERM scenario as covered in Section 15.2. This is a prerequisite for the SAP Risk Management solution setup.

The first pillar of the Basel II Capital Accord deals with maintenance of regulatory capital calculated for three major components of risk that a financial institution faces: credit risk, operational risk, and market risk. Capital requirement refers to the standardized requirements in place for
banks and other depository institutions, which determines how much capital is required to be held for a certain level of assets through regulatory agencies such as the Bank for International Settlements, Federal Deposit Insurance Corporation (FDIC), or Federal Reserve Board. These requirements are put into place to ensure that these institutions aren’t participating or holding investments that increase the risk of default and that they have enough capital to sustain operating losses while still honoring withdrawals. This is also known as regulatory capital. There are three different approaches used to determine regulatory capital requirements for operational risk: basic indicator approach (BIA), standardized approach (STA), and the internal measurement approach (an advanced form of which is the advanced measurement approach [AMA]).

The model described in Tables 15.14 and 15.15 provide a recommendation for customers based on their external versus internal requirements, size of the institution, and the capital determination method being used. Note that this is simply a recommendation, and customers can choose to ignore the model and/or use a hybrid approach.

<table>
<thead>
<tr>
<th>External Regulatory Requirements</th>
<th>Internal Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Indicator Approach (BIA)</td>
<td>Standardized Approach (STA)</td>
</tr>
<tr>
<td>Simple static data management (organization and risk category hierarchies)</td>
<td>Advanced static data management (views and dependent hierarchies)</td>
</tr>
<tr>
<td>Loss event management</td>
<td>Loss event management</td>
</tr>
<tr>
<td>Analytics</td>
<td>RCSA and surveys</td>
</tr>
</tbody>
</table>

Table 15.14: Small Financial Institution Implementation Model Comparison

After you’ve reviewed and chosen the best implementation model, you naturally shift your focus to the solution implementation. The implementation process used is the same as shown earlier in Figure 15.2. Similar to our approach in Section 15.2, we’ll only focus on the business blueprint stage that captures customer requirements for the ORM scenario.

### 15.4.1 Business Blueprint

The objective of this most critical phase of the project is to understand the customer’s ORM process and business requirements. The business blueprint document captures the customer’s business requirements, mapping the requirements to solution functionality, along with details
about system configuration and data setup. The business blueprint is developed in close consultation with the business users and serves as a reference scope document for the solution implementation.

Next, we describe how to complete the several blueprinting tasks before we launch into the realization phase of our implementation of ORM. In the following sections, we’ll review:

- Solution configuration
- Master data setup
- Loss event management workflow and upload
- Reporting

Let’s look at each of these elements of the blueprinting phase for ORM in further detail.

### 15.4.2 Solution Configuration

In the solution configuration task, the customer business requirements are mapped to the SAP Risk Management Customizing Implementation Guide (Transaction SPRO). The parent Governance, Risk, and Compliance node in the IMG specifies customizing entries for all GRC solutions. The IMG entries for the OPERATIONAL RISK MANAGEMENT FOR BANKING INDUSTRY section as shown in Figure 15.27 under the Risk Management node are required to be set up. These IMG entries define configuration for Loss Event Management attributes and workflow, Risk Control Self-Assessments setup, and Aggregation score and color settings. Documentation and usage details for each IMG entry is available as part of Transaction SPRO.

### 15.4.3 Master Data Setup

Next, let’s look at the master data requirements for the customer. For ORM, the four primary master data entities are ORGANIZATIONS, RISK CATEGORIES, PROCESSES, and PRODUCTS. These entities are available in the MASTER DATA work center on the portal as shown in Figure 15.28.
Now let’s look at each of these four entities in further detail and see how customer requirements can be captured and mapped in the solution.

Organizations

Organizations can have a master or management structure and one or more dependent structures (Basel II view, Legal view, Audit view, Business Line view, ORX view, etc.). Customer requirements for the master and dependent structures, including the mapping, are captured in the business blueprint. Figure 15.29 shows a sample of how customers may define their requirements.

Both the master and dependent organization structures are captured using the ORGANIZATIONS quick link under the ORGANIZATIONS section shown earlier in Figure 15.28. Open the ORGANIZATIONS quick link to view the organizations master data. A sample is shown in Figure 15.30. At the top, the View dropdown selection is set to MANAGEMENT HIERARCHY. This view is the master organization structure.

The dependent structures are set up as organizational views. Figure 15.31 shows the ORX dependent structure view, and Figure 15.32 shows the Basel II dependent structure view.
In addition to capturing the master and dependent organization structures, the entities need to be mapped between these structures. The mapping enables reports and analytics to find and pull the appropriate loss and risk information for the dependent structures. This mapping is done using the Master and Dependent Organization Views Mapping quick link under the Organizations section shown earlier in Figure 15.28. Open the Master and Dependent Organization Views Mapping quick link to define this mapping as shown in Figure 15.33.

In Figure 15.33 the Private Banking node of the master organization structure is mapped to the Retail Banking node of the Basel II dependent organization structure.

Risk Categories

Similar to organizations, risk categories can also have a master or management structure and one or more dependent structures (Basel II view, Business Line view, ORX view, etc.). Customer requirements for the master and dependent structures, including the mapping, are captured in the business blueprint. Figure 15.34 shows a sample of how customers may define their requirements.

Both the master and dependent risk category structures are captured using the Risk Catalog quick link under the Risks and Responses section shown earlier in Figure 15.28. Open the Risk Catalog quick link to
view the risk category master data. A sample is shown in Figure 15.35. This common master data entity captures risk categories and risk templates for the entire solution. The master and dependent structures are set up as different parent nodes under the classification hierarchy. The Is Secondary Top Node attribute of a parent node distinguishes between master and dependent structures.

The Is Secondary Top Node attribute is set as ‘No’ for master structures. The Operational Risk structure as shown in Figure 15.35 is a master structure as the Is Secondary Top Node attribute is set as ‘No’. In fact, all nodes except the VOEB node in Figure 15.35 are master risk category structures. Here you see several nodes—both the ERM and the ORM scenarios in this solution—have been implemented.

Figure 15.35 shows the VOEB structure, which is a dependent risk category, as the Is Secondary Top Node attribute is set as ‘Yes’. In addition to capturing the master and dependent risk category structures, the entities need to be mapped between these structures. The mapping enables reports and analytics to find and pull the appropriate loss and risk information for the dependent structures. This mapping is done using the Master and Dependent Risk Classification Hierarchies Mapping quick link under the Risks and Responses section shown earlier in Figure 15.28. Open the Master and Dependent Risk Classification Hierarchies Mapping quick link to define this mapping as shown in Figure 15.37.

In Figure 15.37, the External Fraud node of the Operational Risk category structure is mapped to the External Events node of the VOEB dependent risk category structure.
Processes and Products

Processes and products have a single master structure and don’t have dependent structures. Customer requirements for the processes and product structures are captured in the business blueprint. Figure 15.38 shows a sample of how customers may define their requirements.

Both the process and product structures are captured using the Activity Hierarchy quick link under the Activities and Processes section shown earlier in Figure 15.28. Open the Activity Hierarchy quick link to view the activity hierarchy master data. A sample is shown in Figure 15.39. At the top, the Show dropdown is set to Business Processes. Hence, you see the processes structure.

The product structure can be set up as another type of activity hierarchy. Figure 15.40 similarly shows the Products/Services structure.

Now that the master data business requirements are captured, let's review a few details about loss event management, which is the cornerstone of ORM. Losses are part of the transactional data, but from a blueprint perspective, a couple items need to be captured.
First the loss event management workflow needs to be set up. The loss event management workflow is very flexible and adaptable for all customer requirements. This workflow is set up in the IMG customizing entries (Transaction SPRO). The Solution Configuration section describes the list of IMG entries to be set up. The Define Loss Event Types and Workflow Configuration, as shown earlier in Figure 15.27, captures the loss event workflow configuration.

Customers will also have historical loss information that needs to be uploaded into SAP Risk Management. Customers may also choose to periodically upload additional loss information even after go-live.

Hence, the blueprint document must capture the customer’s loss information to be uploaded into the system.

Loss event management, including upload, is done using the Assessments work center as shown in Figure 15.41. The quick links under the Loss Event Assessments section are used to manage loss events.

Use the Upload Loss Events quick link as shown in Figure 15.42 to upload loss events. An upload file in the Microsoft Excel or XML format needs to be used. The guided procedure checks the content, uploads the data, and confirms the results.
To obtain the file format for loss event upload, use the Loss Event Management quick link to manually enter a few loss events. Then use the Download button with the Download loss event data in QRR Excel option as shown in Figure 15.43. The Excel file obtained with this download operation has the format to use for uploading new loss events.

Figure 15.42 Upload Loss Events

Finally, let’s consider the ORM reporting business requirements. As recommended when we discussed the customer adoption model, it’s best to start by using the standard reports and analytics available under the Reports and Analytics work center as shown in Figure 15.44.

Figure 15.43 Download Loss Events

Figure 15.44 Reports and Analytics Work Center

15.4.5 Reporting

Finally, let’s consider the ORM reporting business requirements. As recommended when we discussed the customer adoption model, it’s best to start by using the standard reports and analytics available under the Reports and Analytics work center as shown in Figure 15.44.
ORM reports are available through the quick links under the Loss Event Reports section in Figure 15.44. The first three quick links—Loss Event Matrix Analysis, Loss Event Overview, and Loss Event Structure—are dashboards. The other links show standard reports.

In Section 15.4.1, we outlined the business blueprint process for implementing and configuring the ORM scenario. The blueprint document is then used to configure the solution, set up master data, set up loss events workflow, and upload loss events and user authorizations, and develop custom reports if necessary. After this is complete, the implementation goes through user acceptance testing. Modifications are made to the implementation based on the outcomes from the user acceptance testing. After users sign off on the readiness of system setup, the installation is replicated to the production environment and use of ORM commences.

If there are subsequent phases in ORM implementation or the customer advances to the next stage in the adoption model outlined in the beginning, the same process should be repeated.

15.5 Summary

As the business landscape grows more complex and global, supply chains become more distributed, and the practice of risk management is evolving from spreadsheets and silos to an enterprise-level process. Companies are starting to align risk management with business value drivers and in the process aren’t only effectively managing risks but also using risk information in decision making and to improve business performance.

SAP Risk Management helps companies automate the process of ERM to preserve and grow business value. Continuous risk insight coupled with the ability to act on emerging risks and opportunities helps companies avoid catastrophic losses, manage risks within established risk appetite levels, and gain advantage from opportunities.

Financial institutions can leverage SAP Risk Management’s operational risk capabilities in addition to ERM to reduce risk of loss resulting from inadequate or failed internal processes, people and systems, or external events. ORM enables companies to comply with external reporting requirements as well as additional internal requirements to manage and monitor performance.

In the next chapter, we’ll cover trade compliance and financial risk.
## Contents

Preface .................................................................................................................. 19
Acknowledgments ................................................................................................. 23

### 1 SAP Governance, Risk, and Compliance Overview

1.1 SAP GRC Suite Overview and Components ............................................. 28  
1.1.1 Value of the Suite as a Whole .............................................................. 29  
1.1.2 Reasons to Implement SAP GRC ......................................................... 30  
1.1.3 SAP Access Control ........................................................................... 31  
1.1.4 SAP Process Control .......................................................................... 41  
1.1.5 SAP Risk Management ....................................................................... 49  
1.1.6 SAP Global Trade Services and SAP Nota Fiscal Electronica .......... 54  
1.2 Shared Master Data .................................................................................. 66  
1.3 SAP Content Life Cycle Management ...................................................... 67  
1.4 SAP GRC 10.0 Architecture and Landscape .......................................... 69  
1.4.1 Backend System Requirements ......................................................... 69  
1.4.2 Two-Tier versus Three-Tier Landscapes ........................................... 72  
1.4.3 Frontend Options ................................................................................ 73  
1.5 Summary ................................................................................................... 74

### 2 Planning SAP GRC Implementations

2.1 Regulations and Policies in SAP GRC ....................................................... 76  
2.1.1 Japan’s J-SOX ..................................................................................... 77  
2.1.2 Australia’s CLERP-9 .......................................................................... 78  
2.1.3 Canada’s C-11 .................................................................................... 78  
2.1.4 Basel II ................................................................................................ 78  
2.2 Purpose of SAP GRC Tools .................................................................... 79  
2.3 Business Processes and Controls ............................................................. 81  
2.4 Organizational Hierarchy and Local Controls ......................................... 82  
2.5 User Interface and Work Center ............................................................... 85  
2.6 Rules ......................................................................................................... 87  
2.7 Reporting .................................................................................................. 87  
2.8 Summary ................................................................................................... 90
3 SAP Access Control Overview ........................................ 91
3.1 General Assumptions during Implementation .......... 92
3.1.1 SAP NetWeaver Business Client as SAP Access
        Control User Interface ........................................ 94
3.1.2 SAP NetWeaver Business Client Use Case .......... 96
3.2 SAP Access Control—Post-Installation Technical
       Settings ........................................................................ 98
3.2.1 Basis Preliminary Check ........................................ 99
3.2.2 Activating BC Sets ............................................. 105
3.2.3 Activate Common Workflow .............................. 110
3.2.4 Workflow Verification ......................................... 117
3.2.5 Troubleshooting for Task-Specific
       Customization ................................................................ 124
3.2.6 Shared Configuration of SAP GRC Systems ... 130
3.2.7 SAP Crystal Reports Features ......................... 137
3.2.8 Activate Profile of Roles Delivered by SAP .... 138
3.2.9 Creating the Initial User in the ABAP System ... 140
3.3 SAP Access Control Configuration ......................... 142
3.4 Summary ................................................................. 144

4 Emergency Access Management Overview ............... 147
4.1 Using Emergency Access Management .................... 149
4.2 Emergency Access Management Configuration
       in SAP GRC ................................................................. 152
4.2.1 Configuration Parameters ................................ 152
4.2.2 General Configuration Steps ............................. 153
4.2.3 Email Configuration ............................................. 157
4.3 Using a Firefighter ID .............................................. 159
4.4 Reporting ................................................................. 161
4.4.1 Consolidated Log Report .................................... 162
4.4.2 Reason Code and Activity Report ...................... 165
4.4.3 Firefighter Log Summary Report ....................... 165
4.4.4 Invalid Emergency Access Report .................... 166
4.4.5 Transaction Logs and Session Detail ................. 166
4.4.6 SOD Conflict Report for Firefighter IDs ........ 166
4.4.7 Reason Code Usage Frequency ....................... 167
4.5 Summary ................................................................. 168

5 Access Risk Analysis Overview ............................... 169
5.1 Access Risk Analysis Basic Configuration .......... 172
5.1.1 Maintaining SAP Access Control Risk Analysis
       Configuration Parameters ....................................... 173
5.1.2 Adding a Connector to the AUTH Scenario ...... 175
5.1.3 Risk Loading and Activation .............................. 176
5.1.4 Synchronization Jobs ........................................ 183
5.1.5 Rule Set Maintenance ........................................ 184
5.1.6 Maintain Shared Master Data ......................... 188
5.1.7 Perform Batch Risk Analysis ......................... 190
5.2 Access Risk Analysis Reporting ............................ 193
5.3 Risk Remediation Process ..................................... 196
5.3.1 Role Cleanup Process with Access Risk
       Analysis ...................................................................... 197
5.3.2 Risk Mitigation as Remediation ....................... 198
5.4 Alert Monitoring ..................................................... 200
5.5 Risk Terminator ..................................................... 200
5.5.1 Configuration Setup in the SAP GRC System .... 201
5.5.2 Configuration Setup in the Plug-In System .... 201
5.6 Access Risk Analysis 10.0: Additional Features ..... 202
5.6.1 Initial Access Risk Assessment ......................... 202
5.6.2 Additional Reporting Features ....................... 202
5.7 Summary ................................................................. 204

6 Business Role Manager Overview ............................ 205
6.1 Business Role Manager Configuration .................... 207
6.1.1 Activation of BC Sets ....................................... 208
6.1.2 Verifying Default Configuration Parameters .... 209
6.1.3 Maintain Role Type Settings ......................... 212
6.1.4 Specify Naming Conventions ......................... 213
6.1.5 Standard Role Methodology ......................... 217
6.1.6 MSMP Workflow Configuration .................... 219
6.1.7 Creating Role Owners ..................................... 222
6.2 Business Role Manager Use: Creating a New
       Single Role ................................................................. 223
6.2.1 Assigning Authorizations to the New Role .... 224
6.2.2 Analyzing Access Risks and Remediation ........ 226
6.2.3 Request Approval ............................................... 227
6.2.4 Role Generation .................................................. 227
6.2.5 Testing the Role .................................................... 228
6.3 Role Maintenance and Reporting ............................... 229
6.4 Summary ..................................................................... 230

7 User Access Management Overview ............................. 231
7.1 Different User Roles in User Access Management ......... 234
7.1.1 General Users ....................................................... 234
7.1.2 Requestors ............................................................ 235
7.1.3 Approvers ............................................................ 235
7.1.4 Administrators ...................................................... 236
7.1.5 Auditors ............................................................... 236
7.2 Maintenance of Users ................................................. 237
7.3 User Access Management Configuration ..................... 237
7.3.1 Basic Requirements .............................................. 238
7.3.2 Activation of Business Configuration (BC) Sets ....... 239
7.3.3 Configuration Parameters ..................................... 240
7.3.4 Maintain Connector Settings .................................. 241
7.3.5 Maintain Data Sources Configuration ..................... 245
7.3.6 Define Request Type ............................................. 247
7.3.7 Maintain Number Range Intervals for Provisioning Requests .......... 248
7.3.8 Define Number Range for Provisioning Requests ............ 249
7.3.9 Maintain End User Personalization ......................... 249
7.3.10 Maintain Provisioning Settings .............................. 251
7.3.11 Maintain User Defaults ....................................... 253
7.3.12 Activate End User Logon ..................................... 253
7.4 Configure the MSMP Workflow ................................. 255
7.5 Process Details: Change/Create Access Request ............ 259
7.5.1 Role Availability for Provisioning ............................ 261
7.5.2 Access Request Process Steps ............................... 262
7.6 Password Self-Service ............................................. 263
7.6.1 Maintain Password Self-Service ............................ 263
7.7 User Access Management Reporting ........................... 265
7.8 Summary ..................................................................... 268

8 SAP Access Control Advanced Topics .......................... 269
8.1 Multistage Multipath (MSMP) Workflow ..................... 270
8.1.1 Configure Process and Global Setting ..................... 271
8.1.2 Maintain Rules and Rule Results ................................ 274
8.1.3 Maintain Agents .................................................. 278
8.1.4 Variables and Templates ....................................... 281
8.1.5 Maintain Paths and Assign Stages to Path ................ 282
8.1.6 Maintain Stages ................................................... 284
8.1.7 Maintain Stage Task Settings ................................. 286
8.1.8 Notification Settings ............................................. 289
8.1.9 Maintain Route Mapping ...................................... 290
8.1.10 Generate Versions ............................................ 291
8.2 Debugging MSMP ..................................................... 293
8.3 Business Rule Framework Plus (BRF+) ......................... 295
8.3.1 BRF+ Use Case in SAP Access Control ................... 296
8.3.2 Chaining Routing Rules Using a Function Module and BRF+ .......... 305
8.3.3 BRF+ Function in Business Role Manager ............... 306
8.4 Workflow Notification Maintenance in MSMP ............... 310
8.4.1 Available Notification Templates ............................ 310
8.4.2 Notification Variables ......................................... 317
8.5 Customizing Workflow Processes: Email Notifications .... 320
8.5.1 Creation of Custom Document Objects ..................... 320
8.5.2 Associate Custom Document Object with Message Class .......... 321
8.6 Select Notification Templates and Recipients ................ 323
8.7 Setting Up Email Reminders ..................................... 325
8.8 Periodic Reviews ..................................................... 326
8.8.1 Configuration for SoD Review ............................... 328
8.8.2 Maintain Reviewers and Coordinators ..................... 330
8.8.3 Generate Data for SoD Review .............................. 332
8.9 HR Triggers ........................................................... 338
8.10 Summary .............................................................. 340

9 SAP Process Control Overview .................................... 341
9.1 The Evolution of SAP Process Control ......................... 342
9.2 SAP Process Control Features .................................... 342
Contents

9.2.1 Date Validity ...................................................... 343
9.2.2 Views ................................................................. 344
9.3 Architecture ......................................................... 344
9.3.1 Installation and Setup ........................................... 346
9.4 Configuration and Basic Settings ......................... 347
9.4.1 General Settings ............................................... 349
9.4.2 Shared Master Data Settings .............................. 356
9.4.3 SAP Process Control Reporting ......................... 357
9.4.4 Common Component Settings for SAP Process Control ......................................................... 358
9.5 Implementation Overview of SAP Process Control ...... 360
9.5.1 Setting Business Goals ........................................ 361
9.5.2 Phased Approaches ............................................ 361
9.5.3 Master Data Collection ....................................... 363
9.5.4 Process Control Users and Roles ......................... 363
9.6 Overview of SAP Process Control Usage ................... 364
9.6.1 Documenting .................................................... 365
9.6.2 Scope .............................................................. 365
9.6.3 Evaluation ........................................................ 366
9.6.4 Monitoring and Remediation ............................... 366
9.6.5 Reporting ........................................................ 367
9.6.6 Certification ..................................................... 368
9.6.7 Policy Management .......................................... 369
9.7 Summary ............................................................. 369

10 SAP Process Control Master Data ................................. 371
10.1 Organizations ..................................................... 374
10.1.1 Multiple Hierarchies ........................................ 376
10.1.2 Validity Dates and Time Frames in the Organization Structure ........................................... 377
10.2 Business Process Models ........................................ 378
10.3 Regulations ........................................................ 382
10.4 Policies .............................................................. 384
10.5 Accounts and Account Groups .............................. 385
10.6 Master Data Content Management and Transport .......... 387
10.6.1 Master Data Upload Generator ........................... 388
10.6.2 Content Lifecycle Management ........................... 391

10.6.3 CLM versus MDUG ........................................... 393
10.7 Summary ............................................................. 394

11 Continuous Controls Monitoring ................................. 397
11.1 Continuous Monitoring Architecture ....................... 398
11.2 Configuring Continuous Control Monitoring .......... 402
11.3 Creating Data Sources .......................................... 409
11.3.1 Adding Data Source Information ......................... 411
11.3.2 Defining the Technical Details ............................ 413
11.3.3 Pointing to a Connector ..................................... 415
11.3.4 Adding Documentation ...................................... 417
11.4 Creating Business Rules ........................................ 418
11.4.1 Basic Information .............................................. 421
11.4.2 Filter Criteria .................................................... 422
11.4.3 Deficiency Criteria ............................................ 423
11.4.4 Conditions and Calculations ............................... 425
11.4.5 Technical Settings and Monitoring Rule Behavior ......................................................... 426
11.4.6 Ad Hoc Query ................................................... 426
11.5 Data Source Types and Related Rules ....................... 427
11.6 Assigning Rules to Controls .................................... 430
11.7 Scheduling Monitoring Rules .................................. 431
11.8 Structured Approach to Continuous Controls Monitoring ......................................................... 434
11.8.1 The Nature of ERP Controls ............................... 435
11.8.2 The Goal of Monitoring ...................................... 436
11.8.3 Effective Monitoring .......................................... 437
11.8.4 The Importance of Proper Configurations and Master Data Settings ................................... 438
11.8.5 Transactions .................................................... 439
11.8.6 Reports and Analytics ........................................ 440
11.9 Summary ............................................................. 441

12 Continuous Controls Monitoring: Data Source Types ......................................................... 443
12.1 Configurable Data Sources and Rules ....................... 444
12.1.1 Configurable Data Sources .................................. 445
17 Compliance with Environment, Health, and Safety Management ........................................... 625

17.1 Integration of SAP EHS Management and SAP Global Trade Services ......................... 626
17.1.1 SAP EHS Management Configuration ......................................................... 628
17.1.2 SAP Global Trade Services Configuration ................................................. 636

17.2 Visualization Features with SAP GTS 10 ............................................................... 642
17.2.1 Accessing the New User Interface ............................................................... 643
17.2.2 SAP NetWeaver Business Client (NWBC) .................................................. 644

17.3 Sanctioned Party List Screening Configuration ......................................................... 645

17.4 SAP Global Trade Services Deployment and Reporting ........................................... 647
17.4.1 Deployment Options ................................................................................. 648
17.4.2 Reporting ............................................................................................... 649
17.5 Summary ....................................................................................................... 656

18 Supply Chain Compliance .......................................................................................... 657

18.1 Import Filing to Reduce Compliance Costs ............................................................. 658
18.2 Import Processes within SAP ERP ......................................................................... 658
18.3 SAP Global Trade Services Declarations ................................................................... 660
18.3.1 Customs Document Review ......................................................................... 661
18.4 Customs Import Process Configuration with SAP ERP .......................................... 668
18.5 SAP Global Trade Services Configuration ............................................................ 673
18.6 Configuration Settings for SAP Customs Management ............................................ 681
18.7 Summary ....................................................................................................... 694

19 Conclusion ............................................................................................................. 695

19.1 Chapter Review ............................................................................................... 696
19.2 Business Benefits of the GRC Suite ...................................................................... 697
19.3 GRC Suite and their Value .................................................................................. 698
19.4 SAP GRC Future Outlook .................................................................................... 699

The Authors .............................................................................................................. 701
Index ......................................................................................................................... 703
## Index

### A

- ABAP Program Data Sources, 464
- ABAP Reports, 464
- ABAP Web Dynpro, 88
- ABAP workflow, 47
- Access Request Approval Workflow, 312
- Access Request Manager, 206
- role owner creation, 222
- Access Risk Analysis, 169, 231
- 10.0 Release, 202
- Alert Monitoring, 200
- background jobs, 192
- connector settings, 175
- Initial Access Risk Assessment, 202
- Mass Mitigation, 199
- mitigation, 198
- Reporting Features, 202
- request types with User Access Management, 248
- results view, 195
- Risk Analysis Framework benefits, 194
- risk owners, 189
- Risk Terminator, 200
- SAP Crystal Report Adapter, 204
- SAP Crystal Reports, 204
- Shared Master Data maintenance, 188
- System-Specific Mitigation, 199
- Access Risk Analysis Tool, 35
- ad hoc query, 426
- Adobe Document Server, 362, 364
- Adobe Document Services, 71, 92
- Advanced Measurement Approach, 564
- agent assignment, 127
- Agent determination, 556
- Anti-bribery Act, 382
- Audit logs, 266
- Authorizations, 352
- automated clearing house, 657
- Automated Monitoring Framework, 406

### B

- Basel II Capital Accord, 52, 561, 563
- Basel III Capital Accord, 52, 561
- Basic Indicator Approach, 564
- Batch Risk Analysis, 190
- Bonded Warehouse, 658
- Boolean value, 472
- Broker Manifest Document, 667
- Business Configuration Sets, 348
- Business process
  - hierarchies, 81
  - model, 81, 378
- Business Role Manager, 205
- BC Sets, 208
- configuration, 207
- configuration of role attributes, 215
- configuration parameters, 209
- Naming Conventions, 213
- Reporting, 229
- Request Approval, 227
- Risk remediation, 226
- Role attributes, 214
- Role Generation, 227
- Role Methodology, 217
- role methodology function, 307
- Single role authorizations, 224
- Single role creation, 223
- Business Role Manager Tool, 38
- Business Rule Framework, 212, 219, 255, 359
- BRF+ Formula, 492
- BRF+ Top Expression, 491
- BRF+ Workbench, 471, 484, 485, 487
- Business Role Manager, 212
- condition groups, 308
- groups, 484
- Initiator rule maintenance, 303
- Routing Rules, 305
- workbench, 299
- Business rules, 418
- categories, 422
Business rules (Cont.)
Creation of, 418
Data source types, 427
Maintenance, 419

C

CCM → Continuous Control Monitoring
Central User Administrator, 206
Change Log Check Rules, 452
Cluster tables, 440
Compliance management plans, 43
Connection Settings, 135
Content Lifecycle Management, 391
Continuous Control Monitoring, 380, 397, 443, 457, 467, 503
Authorizations, 515
Binding parameter values, 503
Business Rules, 505
Change Logging, 465
Control rule assignment, 433
Data security, 515, 516
Data Security models, 521
Data Sources, 504
Import and export, 358
Operational Data Provider (ODP) Rules, 468
Regulation selection, 433
Security, 516
Security model, 521
test schedules, 514
Continuous Monitoring Scheduler, 513
Controls
Assigning rules, 430
ERP, 435
Correctness, 45
Cost Accounting Standards, 635
Credit risk, 563
Cross-Plant Preference Model, 614
custom document objects, 326
customs bond, 657
Customs Declarations, 597
Customs Management, harmonized tariff number structure, 679

D

Data Source Types, 410, 427
ABAP reports, 428
Events, 429
External partner, 429
Integration, 429
SAP HANA Virtual Data Model, 428
SAP NetWeaver BW query, 428
datamart, 367
Date Validity, 343, 354, 367
effective dates, 343
Deficiency Analysis Types, 424
Deficiency conditions, 505
Deficiency fields, 456, 481
Determination Procedure, 637, 639
document object, 314
document types
billing, 613
sales, 613
Duty drawback, 593
Duty rates, 596

E

Electronics Compliance Reporting, 65
Email Reminders, 325
Embargo check, 58
Event Type Linkage, parameter settings, 127
Export legal control, 58
External Partner Data Sources, 464

F

False positives, 185, 198
Firefighter ID, 90, 148
Foreign trade organization (FTO), 681
Fraud detection, 434

G

Generally Accepted Accounting Principles, 76
Globally Unique IDs, 359, 499

H

Harmonized Tariff System, 596
Hazardous service check, 641
Hierarchies
Parallel, 376
Simple, 379
HR authentication
Personnel numbering, 246
Social Security number, 246
HR Triggers, 348

I

Implementation
Business Blueprint, 529
Data conversion, 532
Solution configuration, 529
Import legal control, 58
Import management, 658
Import Master Declaration Document, 667
Integration scenarios, 135
Internal controls, 434
International Financial Reporting Standard, 76
Intra European Community Trade Statistics, 65

J

Job Monitor, 402
Join conditions, 447

K

Key Performance Indicators, 49

L

LDAP, 235
directories, 360
Server, 359

Legacy Automated Monitoring, 402
Letter of Credit, 63
Lightweight Directory Access Protocol, 82, 235
Limit values, 631
Loss event management, 575

M

Market risk, 563
Master Data Upload Generator, 387, 496, 550
MDUG, 357, 387
Message classes, 326
Mitigation controls, 198
Monitoring, 397
API, 462
Backend systems, 434
Business goals, 436
Change log rules, 439
Control design assessments, 366
Logic, 477
Master data, 439
Rule Behavior, 426
Rules, 437
rules, scheduling, 431
Transaction, 439
MSMP, 219
Agent maintenance, 278
Available Notification Templates, 310
BC sets, 110
Configuration, 219
Configuration and Global Settings, 271
Custom Document Object, 321
Custom Document Objects, 320
Debugging, 293
Maintenance, 255
Message class, 311
Notification Settings, 289
Paths and path stages, 282
Route Mapping, 290
Rules and Rule Results, 274
Stage maintenance, 284
Stage task settings, 286
Variables and Templates, 281
Version generation, 291
Index

MSMP (Cont.)
Workflow Notification Maintenance, 310
Workflow Processes Email Notifications, 320
Multistage Multipath Workflow, BC Set activation, 255

N
New Agent fields, 279
North America Free Trade Agreement, 598
Notification Templates, 323
Notification Variables, 317
Number ranges
customs documentation, 606
internal, 606
preference models, 607
vendor declarations, 606

O
OLSP, 506
Online Transactional Processing, 49
OpenSQL, 440
Operational Data Provider (ODP)-based monitoring, 467
Operational Risk Management, 52, 563
Business Blueprint, 565
implementation scenario, 563
Loss Event Management Workflow, 576
mapping structures, 570
Master Data Setup, 566
organizational structures, 568
Organizations, 568
Processes and Product structures, 574
Risk Categories, 571
risk category structures, 573
Solution Configuration, 566
Order to Cash, 48
organization views, 357
organizational hierarchies, 374, 430
organizational structures, 374
Organizational-Level System Parameters, 506, 507

P
Parameter group, 142, 209
Periodic Reviews, 326
Personal Object Worklist
Personalization, 355
Work inbox, 354
Plant-Based Preference Model, 614
preference determination, 671
process hierarchy, 430
process node, 379
Product classification, 57
Property tree data transfer, 634
Provisioning
direct, 251
indirect, 251
settings, 251
System-specific, 253

Q
Query Designer, 468
Query lookup, 415

R
Regulations, 372, 382
Regulatory compliance, 434
hierarchies, 382
List Management, 636
Lists, 635
Regulatory capital, 564
advanced measurement approach, 564
basic indicator approach, 564
internal measurement approach, 564
standardized approach, 564
regulatory modeling, 371
remediation plan, 516
Remote function call, 240
RFC destination, 406
Risk Analysis Framework, 193
Risk Assessments, 552
Risk Management, partner group configurations, 617
Risk Remediation, 193, 196
Mitigation, 194
SoD risk analysis, 196
Role Maintenance, 229
Root Organization Hierarchy, 84, 374
rule definition, 449
rule sets, 184
S
Sanctioned Party List, 643, 645
Sanctioned Party List Screening, 58, 588
SAP Access Control, 34
10.1 Release, 150, 261, 460
Administrator role, 188
Basis team role, 142
BC Set naming conventions, 106
BC Sets, 105
BRF+ Use Case, 296
Business Role Manager, 206
Business Rule Framework Plus, 295
Common workflow, 110
Email configuration, 157
Initial User, 140
Multistage Multipath (MSMP) Workflow, 270
predelivered e-mail reminders, 325
Role and profile activation, 139
SAP Access Risk Analysis risk definition process, 185
Rule ID generation, 181
SAP Access Risk Maintenance, risk maintenance, 184
SAP Advanced Planner and Optimizer, 171
SAP Business Explorer, 468
SAP Business Workflow, 352
SAP BusinessObjects Web Intelligence, 468
SAP Compliance Management, 58, 586, 613, 641
Embargo Checking, 588
Import/Export Legal Controlling, 587
Materials Management Integration, 588
Sales and Distribution Integration, 588
Sanctioned Party List Screening, 586
SAP Content Lifecycle Management, 67, 387, 496, 643
SAP Continuous Control Monitoring
Configuration, 402
deficiency criteria, 423
Transactions, 439
SAP Contract Lifecycle Management, Comparison with MDUG, 393
SAP Crystal Reports, 468
Features, 137
SAP Customer Relationship Management, 171
SAP Customs Management, 589, 613
calculation profile for the import, 692
Configuration, 681
task settings for document types, 683
Customs Communication Service, 589
Customs Declaration, 59
customs declaration duty type, 692
Define document types, 682
document type activation, 683
document type assignment, 693
document type mapping, 685
Duty Calculation, 590
incomplete procedure, 686
Item category definition, 685
Map customs declaration and legal regulation, 683
Package type mapping, 690
process template, 688
Product Classification, 590
Trade Document Service, 590
deferred documents, 589
Transit Procedures, 59
SAP Easy Access menu, 648
SAP Emergency Access Management, 147
CONSOLIDATED LOG REPORT, 164
Consolidated Log Report, 162
Firefighter ID owners, 156
Firefighter Log Summary Report, 165
Firefighter workflow synchronization, 158
Invalid Emergency Access Report, 166
job scheduling, 155
log types, 150
SAP Emergency Access Management (Cont.)
OS Command Log, 151
parameter groups, 152
parameter ID, ... regulations and Environment, Health, and Safety, 637

SAP Environment, Health and Safety Management, 61, 625
Alternative RFC Destinations, 640
Dangerous Goods Management, 626
hazardous substance check, 625, 637
Industry Hygiene and Safety, 626
Integration with SAP GTS, 626
Legal Regulation activation, 639
Occupational Health, 626
Online Checks, 633
Product Safety, 626
quantity check, 627
Quantity Limits and Reactions, 631
quantity thresholds, 632
relative quantity limits, 633
volume tracking, 630
Waste Management, 626
SAP Floor Plan Manager, 88
SAP Global Trade Services, 54, 391, 583, 657
administrative unit, 608
Assign the country group, 677
business partner role, 607
Components, 57
condition record, 584
Configuration, 673
Country groups, 609
cross-plant preference model, 601
customs declaration document, 660
Customs Import process, 673
customs values, 665
define partner functions, 673
determination procedure, 678
Ex Works, 597
Hazardous Substance Check, 640
implementation of system time zones, 604
Implementation of units of measure, 604
Import and Export, 54
import customs declarations, 669
Import partner functions, 673
Import processes, 658
key functions, 585
Legal Regulation, 610, 676
legal regulations and Environment, Health, and Safety, 637

SAP Global Trade Services (Cont.)
Legal Regulations for Country Groups, 637
Logistics process integration, 56
NAFTA, 596
partner grouping, 674
plant-specific preference model, 601
Preferential Processing, 62
System Communication with SAP ERP, 606
transaction value, 596
Transit procedures, 60
SAP Global Trader Services, Document transfer with SAP ERP, 600
SAP Governance, Risk, and Compliance Architecture, 69
AS ABAP, 69
Local Controls, 82
Multiple organization views, 131
Organizational Hierarchy, 82
Plug-In Components, 70
Reporting, 87
Rules, 87
Shared Configuration, 131, 132
User Interface, 85
SAP Governance, Risk, and Compliance Integration Framework, 402
SAP HANA, 368, 440, 699
Continuous Control Monitoring, 468
databases, 408
Enterprise Risk Management, 559
Studio, 469
SAP IT General Controls, 34
SAP NetWeaver
7.31 release, 468
BRF+ rule engine, 425
Process Control, 345
query tools, 451
SAP NetWeaver Business Client, 85, 149, 152, 642
Access Risk Analysis application, 181
Client side access, 97
SAP Emergency Access Management use, 160
Server side access, 97
SAP NetWeaver Business Client for Desktop, 95

SAP NetWeaver Business Client for HTML, 94
SAP NetWeaver Business Rules Framework, 467
SAP NetWeaver Business Warehouse, 368, 408, 559, 590
SAP NetWeaver BW InfoCubes, 460
InfoObjects, 460
SAP NetWeaver BW Query, 460, 468
SAP NetWeaver Identity Management, 35, 71
SAP NetWeaver Portal, 85, 97, 133, 642
Access Risk Analysis application, 180
SAP NetWeaver Process Integration, 30, 71, 408, 459, 462
API implementation, 463
SAP Note Fiscal Electronica, 54
SAP Note 1549013, 464
SAP Note 1653464, 465
SAP Operational Risk Management, 523, 560
SAP Policy Management, 361
SAP Process Control, 43, 341
10.0 Policies functionality, 372
10.1 Release, 359, 426, 443, 451, 459, 461, 471, 497, 514
ABAP Program data sources, 459
Account Groups, 372
Accounts, 372
Analysis Types, 455
Architecture, 344
audit trails, 400
Basic Settings, 347
Basis admin role, 452, 453
Business blueprint template, 360
Business process models, 371
Business rule, 359, 485
change log rules, 455
Change logs versus polling, 453
Common Component Settings, 358
Configurable Data Sources, 444, 445
Configurable queries, 445
Configuration, 347
Connector, 415
Customer Specific Menu Maintenance, 350
SAP Process Control (Cont.)
Data Source Types, ABAP Reports, 459
Data Source Types, SAP NetWeaver BW query, 459
data structures, 363
Datamart reporting, 358
Date Validity, 371
Defining Change Log Rules, 454
Disable Link Functionality, 351
Event driven data sources, 459
Event Registry, 461
Event-Driven Data Sources, 461
Expression Builder, 477, 486
External partner sources, 459
General Settings, 349
History of, 342
Key attributes, 352
Language Support, 350
Master data, 357, 371
Master Data Accounts, 385
master data content management, 372
Master Data Upload Generator, 357
Organization structures, 363, 371
Policies, 384
policy group, 384
Policy Management, 369
Polling, 453
Record Table Changes, 351
Release 10.0, 434, 468
Reporting, 357
Reports, Hierarchical, 367
Roles, 363
runtime application, 489
Segregation of Duty Integration, 459, 460
Shared Master Data Settings, 356
Transport Connection, 350
UI Settings, 356
UI Settings, Side panel, 356
Usage Cycle, 365, 366, 367, 368
User Interface, 372
User roles and security, 503
User-Defined Fields, 353
Users, 363
validity periods, 357
Views, 344, 376
SAP Process Control 10.0, 407, 410
SAP Process Control 10.1, 426
SAP Process Control and CCM, 397
SAP Process Control Implementation, Phased Approaches, 361
SAP Purchasing, 478
SAP Query, 418, 421, 429, 444
data sources, 460
SAP Risk Management, 49, 593
Key Risk Indicator, 438
letter of credit, 592
Organizational structures, 613
preference agreement, 612
Preference Agreement configuration, 614
preference management, 592
Preferencing Processing, 593
Preferencing processing, 597
preference processing configuration, 613
restitution, 595
Rule set configuration, 616
Vendor declarations, 617
Vendor Declarations Management, 597
SAP Service Marketplace, 443, 462
SAP Supplier Relationship Management, 171
SAP User Access Management, 156
SAP Visual Intelligence, 468
Sarbannes-Oxley Act, 26, 76, 170, 382
Search, Implicit, 433
Security Exchange Commission, 341
Segregation of Duties, 32, 169
review, 328
review configuration parameter fields, 328
Review master data, 332
Reviewer and Coordinator maintenance, 330
synchronization steps for review, 327
violations, 75
work index notification, 336
Service level agreement maintenance, 329
type determinations, 330
Service Provisioning Markup Language, 133, 180, 253
Shared Master Data, 66
Solvency II, 52, 561
source connector, 405
Standardized Approach, 564
subprocess node, 380
Superuser Privilege Management, 152
Supply chain compliance, 657
T
Tables
Cluster, 450
Pool, 450
time frame frequencies, 352
trade preference, 593
Trade Preference Processing, ERP Setup, 598
Transaction Code
ALT1, 294
GRAC*, 108
GRAC_BATCH_RA, 190
GRAC_DOWNLOAD_RULES, 178
GRAC_REP_OBJ_SYNC, 183
GRAC_SPM, 149
GRACBATCH_MONITOR, 192
GRFNMW_CONFIGURE, 306
GRFNMW_CONFIGURE_WD, 306
GRFNMW_DEBUG_MSG, 294
NWBC, 260
PFEG, 86, 95, 200, 225, 553, 555
SA38, 318
SAP_GPCR_ROLE_APPR, 220
SAPGUI, 489
SCOT, 154, 157
SCR20, 176
SCL3, 456
SE38, 114, 118
SE61, 320
SCF, 246
SICK, 99
SM20, 351
SM36, 358
SM49, 151
SM59, 141
SM69, 151
SPRO, 106, 175, 183, 208, 249, 254, 302, 555, 609, 616
Transaction Code (Cont.)
SQ01/02, 429
SU01, 149, 200, 222, 237, 251
SUIM, 197
SWDD, 128
SWU3, 113
TREX Search, 355
TREX search, 71, 362
U
US Customs and Border Protection, 658
User Access Management, 106, 141, 231, 232, 293
access request role extraction, 261
benefits, 233
Business Configuration Sets, 239
capabilities, 232
Change/Create Access Request, 259
Configuration, 237
Configuration, Basic Requirements, 238
copy requests, 260
data Sources Configuration, 245
End User Login, 253
End User Personalization, 249
end users process configuration, 260
Firefighter ID, 235
firefighter IDs, 248
LDAP Connector Mapping, 241
Model users, 260
Number Range for Provisioning Requests, 249
Parameter groups, 240
Password Self/Service, 263
reporting, 265
Request Type Definition, 247
role attribute customization, 214
Role Availability for Provisioning, 261
Template based provisioning, 250
template based user requests, 260
User Defaults, 253
User roles, 236
Verification checklist, 259
User Access Management role
approver, 235
requestor, 235
Index

User Access Reviews, 327
User provisioning process, 241

V

Validity Dates, 377
Value Check Category, 449, 452
Vendor Declarations Management, 63

W

Vendor Declarations, worklist, 602
Views, 344

Workflows
event-based, 556
planner based, 556
Asokkumar Christian is currently leading the GRC practice of Krypt, Inc. With refined expertise, he continues to lead and successfully implement SAP GRC projects.

D. Rajen Iyer is a founder of product company, Kryaa, and co-founder of a fast growing supply chain solutions company, Krypt, Inc. He is recognized in the industry and by his peers as a supply chain and compliance solutions expert and an entrepreneur for innovative products and services. He is the author of several SAP PRESS titles on supply chain, trade, and logistics.

Atul Sudhalkar is a product manager for SAP’s Governance, Risk, and Compliance group at SAP’s Palo Alto, California, offices. Before SAP, Atul worked as an architect and development manager at PeopleSoft. Atul holds several patents on product ideas he has developed and has several more patents pending in the United States and abroad.

Satyen Paneri is Senior Director for Solutions go-to-market at SAP. In this role, he is responsible for revenue growth, customer success, and portfolio effectiveness for the SAP Governance, Risk, and Compliance (SAP GRC) solutions. Satyen is a contributor to this title.

We hope you have enjoyed this reading sample. You may recommend or pass it on to others, but only in its entirety, including all pages. This reading sample and all its parts are protected by copyright law. All usage and exploitation rights are reserved by the author and the publisher.