This chapter introduces you to role-based access control. This serves as a basis for showing you how a purpose-based separation can be made within the authorization concept by using line organizational attributes and process organizational attributes. Finally, it describes how to make risk definitions and introduce a new risk assessment.
Chapter 7
Authorization Concept

For a long time, authorizations were the only thing many customers thought about when it came to data protection. Of course, a well-defined authorization concept will continue to play an extremely important role in data protection in the future. However, a large number of adjustments to the concepts may be necessary.

This chapter will provide you with a brief introduction to the role-based access control concept (RBAC). This serves as a basis for showing you how a purpose-based separation can be made within the authorization concept by using line organizational attributes (LOAs) and process organizational attributes (POAs). Finally, we’ll describe abstractly how to make risk definitions and introduce a new risk assessment.

7.1 Users and Authorizations: An Introduction

To display how the principle of minimization and purpose limitation can be realized in authorizations, you’ll need at least an overview of users and authorizations. The following explanations are based on the book Authorizations in SAP Software by Lehnert and Stelzner (SAP PRESS, 2010, www.sappress.com/2316).

7.1.1 Users

For a (natural) person to be able to perform actions in the SAP system, he needs a user to whom authorizations are assigned (see Figure 7.1). Each person 1 has 2 a user 3; one (or more) roles 4 are assigned to the user. A role 5 has a menu 6 that contains applications 7. In relation to these applications, authorizations 8 are included in the role. The individual authorizations are of an authorization object 9.
All of the actions in the SAP system are performed by users. There are different user types for different types of actions, as follows:

- **Dialog user**
  Dialog users are personalized for natural persons who use the graphical user interface, SAP GUI, to log on to the SAP system. The dialog user is the main user type and therefore the focus of this book.

- **Service user**
  Service users are used, for example, for the anonymous access of several users in web services. For this reason, the authorizations for this user type should be restricted considerably. A user logs on using the SAP GUI; it’s possible that the user will log on more than once. The status of the password of a service user is always productive, which also means that only a user administrator can change the password.

- **Communication user**
  Communication users are person-related users who log on, not using the SAP GUI, but rather by means of a remote function call (RFC). The user can change the password. The system checks whether the password has expired or is new. Depending on whether the user has logged on interactively or not, the password may have to be changed.

- **System user**
  System users are needed in technical processes, such as batch runs. The user doesn’t log on using the SAP GUI. Multiple logons are possible when working with system users. Passwords don’t have to be changed.

- **Reference user**
  The reference user is a means of simplifying authorization administration. It’s not possible to log on to the SAP system with this user. The reference user is used to pass on authorizations.

The business authorization concept also has to contain information about the users displayed. For reasons of rule conformity, you can only grant technical users the authorizations that are required, which makes it all the more important that this principle applies to all users that allow people to access the system.

### 7.1.2 Authorizations

Authorizations are necessary to start SAP ERP system applications and execute their functions. The following sections explain the structural properties and the use of authorizations in ABAP programs.

ABAP programs include authorization checks to protect the execution of a business function from unauthorized persons. When the programs are executed, the system determines whether the user is allowed to process the application-specific data as required.

To map a business process from the perspective of authorization, you first have to define a parameter for each characteristic value involved in the process. This parameter is called an authorization field. Because several parameters are normally involved in a business transaction, you’ll need to have the right combinations of authorization fields.

These combinations are called authorization objects. An authorization object consists of a maximum of 10 authorization fields and is assigned to an authorization object class. After you assign values to the fields contained in an authorization object, an authorization is created. In the following sections, we’ll look at two examples of authorization objects.

#### Example: Authorization Object M_BEST_EKO

Figure 7.2 shows a simple example of an authorization object M_BEST_EKO (Purchasing Organization in the Purchase Order).
Authorization Concept

The object contains the authorization fields ACTVT (Activity) and EKORG (Purchasing Organization). You can use the authorizations for this object to specify which types of processing (e.g., creating purchase orders) members of a particular purchasing organization can perform within a given application (e.g., purchase order).

ACTVT is one of the most frequently used authorization fields, and appears in objects in very different application areas.

LOAs EKORG (Purchasing Organization) is the field in which you define the purchasing organizations these authorizations should apply to. Chapter 5, Section 5.2.1, already covered the purchasing organization as a line organizational attribute (LOA). At this point, you can also maintain this exact characteristic (and the other LOAs mentioned in Chapter 5) in the authorizations.

Example: Authorization Object M_BEST_BSA

The situation is similar for authorization objects such as M_BEST_BSA (Document Type in Purchase Order), which are suitable for including process organizational attributes (POAs), as previously described in Chapter 5, Section 5.3.

The authorization objects consist of two fields. If you choose to display this authorization object in Transaction SU21 (Maintain Authorization Objects), you’ll see a screen similar to Figure 7.3.

Figure 7.3 Authorization Object M_BEST_BSA

If the authorization objects have been specified, corresponding authorizations will be generated that will always be based on the role in this model. Both authorization objects are used to control which activity is possible, in which purchasing organization, and in which document type. Depending on the complexity of the program, several authorizations will be checked step by step, starting with a start authorization check. The checking sequence of the technical process in Transaction ME21N (Create Purchase Order) is simplified and schematized in Figure 7.4.

Figure 7.4 Authorization check during program execution
Access Restriction via LOAs and POAs

A user is assigned to a person, and roles are assigned to this user. The roles contain authorization objects that—as soon as the role has been generated—constitute the authorizations of the user concerned. A sequence of authorization checks takes place in a number of programs, for example, in business applications. It’s therefore possible to sufficiently restrict the user’s access using LOAs and POAs by differentiating the access in a relevant way.

7.2 Rethinking Organizational Levels

To complete the picture, a few more details about the organizational levels are necessary. For roles, the organizational levels are strong organizational differentiators that are validated in numerous authorizations. In many cases, the organizational levels correspond to the characteristics described in Chapter 5, Section 5.2.1, such as company code or purchasing organization.

The organizational levels available in the system are shown in table USORG (Organizational Levels for the Profile Generator), as shown in Figure 7.5. In principle, authorization fields for organizational levels can also be “raised.” Organizational levels are initially also authorization fields in an authorization object. Their special feature is their status and the possibilities that arise from it. Organizational levels are required for the derivation concept. As you go through the defined organizational levels, you’ll find that not all organizational levels are LOAs as defined in this book.

[Figure 7.4 Authorization Checks in the Program Sequence]

The first check shown in the graphic for S_TCODE (Transaction Code Check at Transaction Start) is also possible for other start authorization objects; the object S_SERVICE (Check at Startup of External Services) is particularly important for SAP S/4HANA because this is required for SAP Fiori apps.
The derivation concept is the central technical vehicle of the authorization concept. The system also recognizes the need to differentiate roles along clear organizational boundaries. As shown in Figure 7.6, roles can be derived from a central reference role that has its own specific organizational level characteristics and LOAs. Assuming there are three legally independent units, these can each be mapped with one set of LOAs; when deriving the roles, these values are entered in the derived role.

As described in Chapter 5, as a general rule, we assume that the purpose of processing personal data is to be considered specifically for a legally independent entity. Accordingly, it’s also important that the organizational model is reflected in the use of the organizational levels. Chapter 12 deals with the control measures that are necessary to achieve this. An essential question in this context is how the organizational levels were defined in the roles.

If, however, you want to start with authorizations as your first step of implementation, you have no other option than to determine the relationships outlined in Chapter 5, Section 5.2.1. This section will also show you where you can evaluate the assignments in the enterprise structure. You’ll have to determine which assignments are maintained and evaluate whether the relationships refer uniquely to a controller (usually the legal person). The controller is usually represented by the company code.

After you’ve traced this assignment, check table USORG (Organizational Levels for the Profile Generator) to see which organizational levels are available for authorizations in your system. The next step requires an actual analysis; you’ll have to examine the actual assignments to the authorizations in table AGR_1252 (Organizational Levels). You should also consider the manual values of these fields in table AGR_1251 (Authorization Data for Activity Group). Together, these two specifications provide information on which line-organizational differentiations currently exist for you in the roles. Entries made to these fields in table AGR_1251 (Authorization Data for Activity group) are also proof that your authorization concept doesn’t comply with the standard.

No Generic Maintenance
Generic maintenance with "*" or comprehensive intervals "0001–9999" aren’t generally useful as a means of differentiation.

Is the Data Processed Separately for Each Purpose?
Our regular discussions with SAP Consulting often deal with the question of whether or not data can actually be processed separately. In such cases, our standard response is that a brief look at the organizational differentiation of roles will provide a rapidly identified and weighty indicator.

7.3 Defining Process Attributes

POAs were already addressed in Chapter 5, Section 5.3. In doing so, we also clarified our assumptions in the process and gradually presented the elements of an exemplary process: customer, order, delivery, and billing.
Authorization Concept

These business objects are regularly protected by relevant authorization objects that allow you to differentiate according to POAs. As an example, refer to authorization object V_VBAK_AAT (Sales Document: Authorization for Sales Document Types) (see Figure 7.7).

Figure 7.7 Authorization Object V_VBAK_AAT (Sales Document: Authorization for Sales Document Types)

Authorizations for handling a sales order are also assigned in SAP ERP Controlling (CO) (e.g., product cost estimate). From a data protection perspective, an application-related solution should be sought; this is achieved using the two authorization objects in Figure 7.8.


With regard to POAs, it’s also important that you’ve already identified the most important POAs in our procedure model because you’ll also need these attributes for blocking and deleting. Likewise, when using the Data Controller Rule Framework, the model should have already been mapped in its essential parts.

Figure 7.8 LOAs and POAs in the Authorization Objects for the Sales Order

An alternative procedure in this case is much more complex, as there are far more possible fields and approaches. However, experience with the customer has shown that a differentiation has usually already been made for purely business-related and internal organizational reasons; this differentiation must be examined and, where necessary, modified.

One possible starting point is again the characteristic value of the roles, which can be analyzed using table AGR_1251 (Authorization Data for the Activity Group). This time, however, it’s not just the small number of organizational levels that need to be considered but rather other numerous...
fields. You can further facilitate your work by describing the respective activities in the fields. For example, you may add the term “Exclude activity” to the field ACTVT.

### 7.4 Authorization Risks

As previously explained in Chapter 1, Section 1.2.4, authorizations must follow the strict principle of data minimization. All access beyond the purpose of processing is a violation of the minimization principle.

#### Data protection perspective

Risks in the authorization system are usually defined and evaluated. The classic approach is ultimately a principle of prohibition, which is simply based on the following principle: a user should not be able to execute certain actions or certain combinations of actions.

The principle of minimization is, however, a principle of requirement. A user should only be allowed to perform actions that correspond to the purpose of processing.

To highlight this (in a simplified way) with quantity structures, consider that of the approximately 60,000 business transactions, several thousand transactions (approximately 2,500 in the SAP Access Control rules) are listed in the classical risk definition logic and are regarded as risky. However, in terms of the minimization principle of data protection, any transaction that is suitable for exposing personal data is a risk if this isn’t needed for the specific purpose. Realistically, this is 20 times the amount.

#### All too risky?

This, however, not only leads to considerable challenges in terms of the amount of risk definitions but also in terms of the number of hits (again simplified). After all, every one of the users in the system deals with personal data in one way or another, and this is precisely what the number of hits would cover. It’s therefore almost worthless to say that almost every user deals with personal data. The question is therefore, what do we have to prove? We have to prove which users have access for which processing purposes.

#### Activity-related risks

From a user authorization perspective, activity-related risks can be divided into three different types of critical access into the system:

- **Segregation of duties (SoD) conflicts**
  
  SoD conflicts are the result of a combination of two activities. For example, the combination of supplier maintenance and order processing is critical. However, depending on rules, procedures, and Customizing settings, an SoD conflict can also be displayed within a transaction if the set of rules stipulates an SoD between entering and releasing a posting. The technical control of these various activities allows for an operation-oriented SoD; that is, a separation of the entry and release processes can be configured.

- **Critical actions**
  
  Critical actions affect a single activity (execution) leading to a risk. Maintaining metadata preferences, for example, is a critical action because it can result in the production system being opened for unauthorized modifications. A critical action is defined as the connection of an application, for example, of a transaction with an authorization object.

- **Critical authorizations**
  
  Critical authorizations are critical in themselves, without the type of access to this authorization needing to be defined already (technical definition: authorization object without connection to a specific transaction). One example is debugging in change mode.

This is what the “classic” risk perspective has to offer! What about the risks based purely on data protection law?

In data protection, the SoD is particularly important for system-related activities, such as the segregation of user administrator and authorization administrator, or the SoD in transportation management.

#### Transportation Management

By transportation management, we mean the management of transport requests between development and production systems.

SoD requirements explicitly linked to business management should be borne in mind, for example, when customers or suppliers are unblocked. The allocation of a special bonus and the initiation of payment are still a risk of SoD in terms of business management; this risk doesn’t have to be subject to any data protection considerations. The risks involved in the
SoD, therefore, play a rather marginal role in data protection in terms of volume.

Critical actions also exist in data protection. Naturally, technical actions are more serious. The previously mentioned general maintenance of metadata preferences is also an explicit data protection risk. Specifically, with regard to data protection, it should also be noted that unlimited access to tables generally constitutes a massive violation of the minimization principle and the principle of purpose separation.

The definition of critical authorizations in data protection is much more important than in classic risk assessment. For example, access to internal vendors (e.g., travel expenses) is a risk for all users, regardless of the type of access, who aren’t explicitly authorized for the purposes relating to internal accounts payable.

The requirement to only provide authorizations if the access is covered from the purpose of the processing leads to a new category. The latter must be in a position to provide information as to whether the separation of purposes in the user’s authorizations has been carried out in such a way that the user only has authorizations resulting from the purposes for which he has to be authorized. The term purpose risk has been introduced to describe this risk.

A purpose risk is a general, purpose-oriented risk definition using the authorization objects assigned to individual artifacts within a purpose, as well as the LOAs and POAs of a purpose. The purpose risk is therefore made up of a set of all critical authorizations as defined by data protection law in relation to all artifacts of a processing purpose.

Let’s begin by taking a look at the graphic in Figure 7.9. In this context, the sales order is protected by two essential authorization objects: V_VBAK_AAT (Sales Document: Authorization for Sales Document Types) and V_VBAK_VKO (Sales Document: Authorization for Sales Areas). The division, distribution channel, or sales organization may be used as LOAs. The POA is the order type. The activity is negligible for this assessment.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>V_VBAK_AAT (Sales Document: Authorization for Sales Document Types)</td>
<td>AUART</td>
<td>Sales Document Type</td>
</tr>
<tr>
<td></td>
<td>ACTVT</td>
<td>Activity</td>
</tr>
<tr>
<td>V_VBAK_VKO (Sales Document: Authorization for Sales Organization)</td>
<td>VKORG</td>
<td>Sales Organization</td>
</tr>
<tr>
<td></td>
<td>VTWEG</td>
<td>Distribution Channel</td>
</tr>
<tr>
<td></td>
<td>SPART</td>
<td>Division</td>
</tr>
<tr>
<td></td>
<td>ACTVT</td>
<td>Activity</td>
</tr>
</tbody>
</table>

Table 7.1 Risk Definition (Combination of “Critical” Authorizations)

This artifact-related observation must now be repeated for each artifact in the purpose until all risks have been defined.
The cumulative total of all risk definitions (which are in fact definitions of critical authorizations) represents the entire purpose risk. Thus, two levels can be represented: one general level that provides information about the purpose, and a concrete level that also identifies the artifacts in relation to the purpose (see Table 7.2).

<table>
<thead>
<tr>
<th>User</th>
<th>Purpose (General Level)</th>
<th>Artifact (Specific Level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Miller</td>
<td>Sale of cough syrup</td>
<td>Customer master, sales order, billing document</td>
</tr>
<tr>
<td>Miller</td>
<td>Sale of peppermint tea</td>
<td>Customer master</td>
</tr>
</tbody>
</table>

Table 7.2 Two Levels of Purpose Risk

Again, if you’ve been following our proposed procedure model, where significant values have already been determined, they must also be applied accordingly. To do this, you’ll have to prepare the artifacts for their SAP ILM objects, for which you’ve already created rules. If you’ve already set up the Data Controller Rule Framework, you’ll find yourself in the comfortable position of having POAs, LOAs, and SAP ILM objects already assigned to the purpose.

7.5 Summary

The topic of authorizations is technical and not necessarily trivial. It’s also important for a more system-remote data protector to know that authorizations are generally checked at several levels, that the line organization and the process organization must be observed, and that there is a close relationship between the rules for deletion and the authorizations. It’s unlikely that a data protector of this kind will make technical risk definitions independently. They might also be able to consult those responsible in IT as to which risks are defined and how POAs and LOAs are to be taken into account.

In this chapter, we’ve shown the authorization-affine IT specialists that they can ultimately—albeit in the guise of data protection—expect a familiar field of activity with a generally substantial need for action.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>15</td>
</tr>
<tr>
<td>Preface</td>
<td>17</td>
</tr>
<tr>
<td>1 Introduction to General Data Protection Regulation</td>
<td>25</td>
</tr>
<tr>
<td>1.1 What Does the GDPR Mean for you?</td>
<td>25</td>
</tr>
<tr>
<td>1.1.1 Conceptual and Factual Principles</td>
<td>26</td>
</tr>
<tr>
<td>1.1.2 An Essential Legal Consideration</td>
<td>30</td>
</tr>
<tr>
<td>1.1.3 Principles of Processing</td>
<td>31</td>
</tr>
<tr>
<td>1.1.4 Special Categories of Personal Data</td>
<td>33</td>
</tr>
<tr>
<td>1.1.5 Justifiable Facts for Processing</td>
<td>35</td>
</tr>
<tr>
<td>1.1.6 Requirement of Transparency</td>
<td>37</td>
</tr>
<tr>
<td>1.1.7 Accuracy of Data</td>
<td>42</td>
</tr>
<tr>
<td>1.1.8 Right to Be Forgotten</td>
<td>42</td>
</tr>
<tr>
<td>1.1.9 Data Portability</td>
<td>45</td>
</tr>
<tr>
<td>1.1.10 Objection, Automated Individual Decision-Making, and Profiling</td>
<td>46</td>
</tr>
<tr>
<td>1.1.11 Appropriateness of Measures, Documentation, and Proof</td>
<td>46</td>
</tr>
<tr>
<td>1.1.12 Security of Processing</td>
<td>47</td>
</tr>
<tr>
<td>1.1.13 Privacy Impact Assessment</td>
<td>51</td>
</tr>
<tr>
<td>1.1.14 Records of processing activities</td>
<td>52</td>
</tr>
<tr>
<td>1.2 Which Requirements Require Technical Support?</td>
<td>53</td>
</tr>
<tr>
<td>1.2.1 Purpose Limitation of Processing</td>
<td>54</td>
</tr>
<tr>
<td>1.2.2 Data Accuracy: Rectification</td>
<td>55</td>
</tr>
<tr>
<td>1.2.3 Data Deletion and Data Blocking</td>
<td>56</td>
</tr>
<tr>
<td>1.2.4 Technical and Organizational Measures</td>
<td>60</td>
</tr>
<tr>
<td>1.2.5 Accountability and Auditability</td>
<td>66</td>
</tr>
<tr>
<td>1.2.6 Right of Access</td>
<td>69</td>
</tr>
<tr>
<td>1.3 Which Requirements Can Be Technically Supported?</td>
<td>72</td>
</tr>
<tr>
<td>1.3.1 Consent</td>
<td>72</td>
</tr>
</tbody>
</table>
3 Implementation Approach

3.1 Project Implementation Steps .................................................. 111
  3.1.1 What is the Inductive Approach? ...................................... 114
  3.1.2 Blocking and Deleting Personal Data as
       Your Starting Point ............................................................. 115
  3.1.3 Separation Based on Purpose .............................................. 118
  3.1.4 Separating the Purpose and Authorizations ..................... 120
  3.1.5 Informing the Data Subject ................................................ 121
  3.1.6 Logging ........................................................................ 122
  3.1.7 Data Transmission Security .............................................. 123
  3.1.8 Technical Security ............................................................. 124
  3.1.9 Data Portability ................................................................. 125
  3.1.10 Audit, Verification, and Documentation ......................... 125

3.2 Record of Processing Activities Approaches .................................. 130
  3.2.1 Inductive versus Deductive Approach .............................. 130
  3.2.2 Where the Two Approaches Meet ...................................... 132

3.3 Summary ............................................................................. 132

4 Blocking and Deletion with SAP Information Lifecycle Management

4.1 Introduction to ILM ................................................................. 133
  4.1.1 Fundamentals of SAP Information Lifecycle
       Management ........................................................................ 134
  4.1.2 Lifecycle Management ...................................................... 136
  4.1.3 Overview of Solutions ..................................................... 140

4.2 Preparatory Steps .................................................................... 143
  4.2.1 Blocking Master Data in Transaction SPRO ...................... 143
  4.2.2 Blocking Transactional Data in Transaction SPRO ........... 149
  4.2.3 Blocking Master Data in SAP Information Lifecycle
       Management ........................................................................ 149
  4.2.4 Archiving Master and Transactional Data ......................... 156
  4.2.5 Destruction of Master and Transactional Data .................. 157

2 Personal Data in SAP Business Suite and
SAP S/4HANA .......................... 81

2.1 SAP Business Suite and SAP S/4HANA Data ................................ 81

2.2 Personal Data in SAP ERP ...................................................... 84
  2.2.1 Business Partner .................................................................. 84
  2.2.2 Direct Personal Data Records in SAP ERP Financials .......... 85
  2.2.3 Further Personal Data Records in SAP ERP Financials ....... 91
  2.2.4 Employee Data in SAP ERP Financials ............................... 92
  2.2.5 User Data ........................................................................ 92
  2.2.6 Direct Personal Data Records in SAP ERP Controlling ....... 93
  2.2.7 Indirect Personal Data Records in SAP ERP Controlling ..... 94
  2.2.8 Reporting Tools in SAP ERP Controlling and Customer-
       Specific Reporting ................................................................. 97
  2.2.9 Direct Personal Data in SAP ERP Sales and Distribution .... 97

2.3 Personal Data in SAP ERP HCM ............................................. 99
  2.3.1 Types of Personal Data ...................................................... 99
  2.3.2 Info Subtypes .................................................................. 102

2.4 Personal Data in SAP CRM .................................................... 103
  2.4.1 Business Partners as Master Data ...................................... 104
  2.4.2 Transactional Data of Business Partners ......................... 106
  2.4.3 Data Exchange with Other SAP Systems ......................... 107
  2.4.4 Report Options for Business Partners in Marketing .......... 107

2.5 SAP Business Suite Technical Integration Example ..................... 108

2.6 Summary ............................................................................. 109

1.4 Summary ............................................................................. 79

1.3.2 Data Minimization ............................................................... 72

1.3.3 Data Accuracy: Data Management ....................................... 74

1.3.4 Advance Information .......................................................... 74

1.3.5 Records of Processing Activities ......................................... 75

1.3.6 Accountability: Compliance Management ............................. 76
4.2.6 Blocking and Deleting Master Data: Application Rule Variants 160

4.3 Blocking from a Business Perspective 168
4.3.1 Blocking Master Data in the Business Process 168
4.3.2 Display of Blocked Master Data in the Business Process 172
4.3.3 Unblocking Master Data in the Business Process 178
4.3.4 Blocking Transactional Data in the Business Process 181
4.3.5 Display of Blocked Transactional Data in the Business Process 182

4.4 Deletion from a Business Perspective 185
4.4.1 Data Destruction from the Database 185
4.4.2 Destruction of Archived Data 188

4.5 Legal Case Management 191

4.6 Time-Based Blocking of Personal Data in Personnel Management 193

4.7 Summary 195

5 Purpose-Based Processing 197

5.1 Controller and Purpose 197

5.2 Organizational Structures (Line Organization) 200
5.2.1 Key Organizational Structures 201
5.2.2 Alternate Structure Arrangements 205

5.3 Process Organizational Structures 206
5.3.1 Account Groups 207
5.3.2 Business Objects in SAP ERP Sales and Distribution 210
5.3.3 Purpose Attributes in Sales Order Processing 213

5.4 How Organizational Structures Define Purpose 214

5.5 Summary 215

6 Data Controller Rule Framework 217

6.1 Data Controller Rule Framework 221
6.1.1 Configuration of the Data Controller Rule Framework 223
6.1.2 Rule Maintenance in the Data Controller Rule Framework 230

6.2 Summary 237

7 Authorization Concept 239

7.1 Users and Authorizations: An Introduction 239
7.1.1 Users 239
7.1.2 Authorizations 241

7.2 Rethinking Organizational Levels 244
7.3 Defining Process Attributes 247

7.4 Authorization Risks 250

7.5 Summary 254

8 Information Retrieval Framework 255

8.1 Transparency: Access to Data and Information 256

8.2 Setup of the Information Retrieval Framework 257
8.2.1 Activating the Business Function 257
8.2.2 Determining the System Status 258
8.2.3 Assignment of Authorizations 259

8.3 SAP ILM Objects in the Information Retrieval Framework 260

8.4 Creating an Information Retrieval Framework Data Model 264
8.4.1 Display Information Retrieval Framework Data Model 264
8.4.2 Selecting a Data Record for the Provision of Information 266
8.4.3 Assigning an SAP ILM Object to a Purpose 268
Index

A
ABAP programs 241
Access 325
Access checks 374
Access control 389
Access restriction 244
Account groups 207, 208
Accountability 377
Accounting documents 220
Accounts 104
Accuracy 32, 42, 74, 126
Activity types 95, 96
Address validation 326
Addresses 105
Advance information 74, 256
Amount values 349
Anonymization 47, 352
API channels 297
configuration 305
Application areas 156
Application Link Enabling (ALE) 148, 389
Application names 148
Application rule variants 152, 160, 161, 163
Archivability checks 141
Archive Development Kit (ADK) 136, 398
Archive files 193
Archived data 156, 158
destruction 188
Archiving objects 156, 218, 261
Argument fields 343, 349
Assignment tables 344
Attribute maintenance 318
Attribution 383
Audit activities 129
Audit area 150, 234
Auditing 66
Authorization check 193, 243, 394
Authorization concept 239, 387
Authorization control 325
Authorization field 241
Authorization groups 89, 146, 157, 230, 395
Authorization objects 159, 241, 248, 252
delement 243
Authorization risks 126, 412
Authorizations 114, 120, 158, 239
assignment 259
critical 251
deactivating 325
dexample 242
Automated decision-making 46, 70
Availability 50, 375

B
Backup and disaster recovery 412
Backward RFC 283
BDLS run 334
Billing document 212
type 213
Billing documents 220
Blocking 45, 56, 115, 138, 168
Blocking indicators 397
Business Add-Ins (BAdIs) 261, 288
Business Address Services (BAS) 399
Business Continuity Management (BCM) 375
Business functions 144
Business Information Provider (BIP) 399
Business Object Repository (BOR) 192
Business objects 210
Business partner management 203
Business partner model 84
Business partners 84, 143, 294, 309
blocking 148
relationships 104
roles 84, 104
Index

Business partners (Cont.)
types ........................................................... 104
Business Planning and Simulation
(BPS) .......................................................... 107
Business Process Library (BPL) ........ 334
Business Process Library Modeler
(BPL Modeler) .............................................. 342
Business processes ........................................ 206, 221
blocking master data ..................................... 168
unblocking .................................................... 178
Business rules ............................................. 232
Business Rules Framework (BRF) ........ 326

C
Central data maintenance ...................... 317
Central instance (CI) ..................................... 282
Change logging .......................................... 122
Check authorization ....................................... 179
Check date period ........................................ 144
Check tables ............................................. 263
Classification ............................................ 105
Client copies ............................................. 335, 337
Client separation ......................................... 198
Clients ...................................................... 201
Code review .............................................. 401
Code scans .................................................. 370
Communication user ................................... 240
Companies .................................................. 202
Company codes ........................................ 201, 225
Compliance management ......................... 76
Condition fields ......................................... 232, 236
Conditions .................................................. 310
Confidentiality ........................................... 377
Configuration validation .......................... 402
Consent .................................................... 36, 37, 356
Consistency ............................................... 338
Contact persons .......................................... 97, 104, 209
Control frame ............................................ 354
Control keys ............................................. 82
Controller .................................................. 29, 118, 197, 221
joint responsibility ....................................... 198
mandatory assignment ................................ 198
Controlling area ......................................... 202
Controlling report ....................................... 94
Controls ................................................... 356, 359
Conversion Workbench (CWB) ................. 343, 350
Conversions ............................................. 334
standard .................................................. 346
Cost Center Accounting .......................... 202
cost center hierarchy .................................. 202
cost centers ............................................... 94, 96
cross-business process search ..................... 282
cross-company code postings ..................... 215
cross-site scripting .................................... 371
Customer data .......................................... 324
Customers ................................................. 89
blocking .................................................... 153, 172
no blocking ............................................... 171

D
Data access control ...................................... 62
Data accuracy ............................................ 364
Data archiving .......................................... 230
Data blocking ........................................... 392
data controller .......................................... 225
Data Controller Rule Framework ............... 120,
122, 126, 128, 217, 221, 246, 249,
279, 382
configuration ............................................. 223
rule maintenance ........................................ 230
data deletion ............................................. 397
data dependency ........................................ 116
data destruction ........................................ 135, 157
data enrichment ........................................ 328
data exchange ........................................... 107
data inventory ........................................... 115
data media control ...................................... 61
data minimization ...................................... 72, 360, 362
Data model errors ....................................... 276
data portability ......................................... 45, 125, 127, 257
data processing ........................................ 28, 142, 200
for employment purposes .......................... 359
Data protection .......................................... 25, 137
data protection impact assessment
(DPIA) ....................................................... 112
Data protection officer ................................ 38
data protector ............................................ 403
data quality assurance ................................ 326
data records ............................................ 266
selection ................................................... 339

Data records (Cont.)
transfer .................................................... 340
Data Retention Rule Framework .................. 120
Data subject requests ............................... 279
data subjects ............................................. 25, 121
data traces ............................................... 349
data transfer ............................................. 114
data transmission security .......................... 123
debtors ..................................................... 89
decentralized data maintenance ................... 316
deductive approach .................................... 112
default audit area ....................................... 229
deletion .................................................... 56, 115, 138, 185
deletion process ........................................ 219
deliveries .................................................. 211, 220
depersonalization ...................................... 43, 49, 363, 391
derivation concept ...................................... 246
destruction worklist .................................... 189
development client ..................................... 333
dialog user ............................................... 240
differential privacy ...................................... 48, 348
distribution channel .................................... 202
division ..................................................... 202
Document Relationship Browser
(DRB) ....................................................... 192
double maintenance .................................... 163
dual control principle .................................. 191
dun & Bradstreet ........................................ 338
duplicate check ......................................... 329
duplicate detection ...................................... 327

Employee data ........................................... 323
Employers ............................................... 104
Encryption ............................................. 49, 391
eop check .................................................. 142, 150, 167
event logging ............................................ 374
external services ........................................ 329
forward RFC ............................................. 283
Frequency of use ...................................... 362

G
General Ledger (GI) .................................... 315
Generic Smart Search (GSS) ...................... 255, 283
Greenfield implementation ....................... 112

H
Health data .............................................. 34

IBAN ....................................................... 295, 361
Identifiable data ........................................ 26
Implementation approach ........................... 111
Inductive approach ..................................... 112, 114
industry solutions ...................................... 144, 340
Info subtypes .......................................... 102
Information .............................................. 114
Information Retention Manager
(IRM) .......................................................... 133
Information retrieval framework ............... 71, 255, 381
confirming changes .................................... 276
correcting data model ............................... 272
create data model ...................................... 264
data model ................................................ 272, 274
define system status ................................... 258
display data model ...................................... 264
set up ...................................................... 257
tables ....................................................... 263
Information sheet ....................................... 106
Infotype namespaces .................................. 100
Infotypes .................................................. 99, 100, 194
country-specific ........................................ 100
Input mask ............................................... 86
Integrity .................................................. 49
Integrity and confidentiality ........................ 369
Interface control ....................................... 383
Interface verification .................................. 127
Intermediate Document (JDoc) ..................... 64
Internal control system .............................. 353
internal orders .......................................... 94
International Financial Reporting
Standards (IFRS) ...................................... 138
IRM rules .................................................. 136, 161
<table>
<thead>
<tr>
<th>Rules (Cont.)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>235</td>
</tr>
<tr>
<td>Runtime</td>
<td>341</td>
</tr>
<tr>
<td>S</td>
<td></td>
</tr>
<tr>
<td>Salaries</td>
<td>96</td>
</tr>
<tr>
<td>Sales documents</td>
<td>220, 228</td>
</tr>
<tr>
<td>Sales order</td>
<td>210</td>
</tr>
<tr>
<td>Sales organization</td>
<td>202</td>
</tr>
<tr>
<td>SAP Access Control</td>
<td>121, 126</td>
</tr>
<tr>
<td>SAP Business Suite</td>
<td>117, 219</td>
</tr>
<tr>
<td>data</td>
<td>81</td>
</tr>
<tr>
<td>technical integration</td>
<td>108</td>
</tr>
<tr>
<td>SAP Business Warehouse</td>
<td>(SAP BW)</td>
</tr>
<tr>
<td>SAP Claims Management</td>
<td>116</td>
</tr>
<tr>
<td>SAP Collections and Disbursements</td>
<td>116</td>
</tr>
<tr>
<td>SAP Customer Relationship</td>
<td></td>
</tr>
<tr>
<td>Management (SAP CRM)</td>
<td>82, 292</td>
</tr>
<tr>
<td>middleware</td>
<td>108</td>
</tr>
<tr>
<td>personal data</td>
<td>103</td>
</tr>
<tr>
<td>Web Client</td>
<td>107</td>
</tr>
<tr>
<td>SAP Enterprise Services</td>
<td>64</td>
</tr>
<tr>
<td>SAP Enterprise Threat Detection</td>
<td>123</td>
</tr>
<tr>
<td>SAP Environment, Health, and Safety (EHS) Management</td>
<td>34</td>
</tr>
<tr>
<td>SAP ERP</td>
<td>81, 107, 282, 319, 348</td>
</tr>
<tr>
<td>personal data</td>
<td>84</td>
</tr>
<tr>
<td>SAP ERP Controlling</td>
<td>93, 94, 248</td>
</tr>
<tr>
<td>SAP ERP Financials</td>
<td>85, 91, 116, 175</td>
</tr>
<tr>
<td>employee data</td>
<td>92</td>
</tr>
<tr>
<td>SAP ERP HCM</td>
<td>99, 203, 335</td>
</tr>
<tr>
<td>master data</td>
<td>100</td>
</tr>
<tr>
<td>SAP ERP HCM Organizational Management</td>
<td>102, 203</td>
</tr>
<tr>
<td>SAP ERP Sales and Distribution</td>
<td>97</td>
</tr>
<tr>
<td>SAP Fiori apps</td>
<td>244</td>
</tr>
<tr>
<td>SAP for Insurance</td>
<td>182</td>
</tr>
<tr>
<td>SAP Gateway</td>
<td>259</td>
</tr>
<tr>
<td>SAP Governance, Risk, and Compliance (SAP GRC)</td>
<td>129, 358</td>
</tr>
<tr>
<td>SAP Information Lifecycle Management (SAP ILM)</td>
<td>92, 120, 122, 126, 133, 210, 217, 254, 255, 393</td>
</tr>
<tr>
<td>action</td>
<td>186</td>
</tr>
<tr>
<td>assign object purpose</td>
<td>268</td>
</tr>
<tr>
<td>blocking master data</td>
<td>149</td>
</tr>
<tr>
<td>objects</td>
<td>150, 221, 232, 260, 273</td>
</tr>
<tr>
<td>overview</td>
<td>134</td>
</tr>
<tr>
<td>rules</td>
<td>227, 228</td>
</tr>
<tr>
<td>search</td>
<td>269</td>
</tr>
<tr>
<td>SAP Landscape Transformation</td>
<td></td>
</tr>
<tr>
<td>Replication Server</td>
<td>64</td>
</tr>
<tr>
<td>SAP Master Data Governance (SAP MDG)</td>
<td>73, 119, 315, 399</td>
</tr>
<tr>
<td>central governance</td>
<td>317</td>
</tr>
<tr>
<td>consolidation</td>
<td>319</td>
</tr>
<tr>
<td>decentralized maintenance</td>
<td>322</td>
</tr>
<tr>
<td>SAP NetWeaver</td>
<td>191</td>
</tr>
<tr>
<td>SAP Patient Management for hospitals</td>
<td>82</td>
</tr>
<tr>
<td>SAP Policy Management (FS-PM)</td>
<td>82, 116</td>
</tr>
<tr>
<td>SAP Process Control</td>
<td>123</td>
</tr>
<tr>
<td>SAP S/HANA</td>
<td>219, 244, 331</td>
</tr>
<tr>
<td>data</td>
<td>81</td>
</tr>
<tr>
<td>SAP Solution Manager</td>
<td>402</td>
</tr>
<tr>
<td>SAP Supplier Relationship Management (SAP SRM)</td>
<td>282</td>
</tr>
<tr>
<td>SAP Supply Chain Management (SAP SCM)</td>
<td>82</td>
</tr>
<tr>
<td>SAP Test Data Migration Server (SAP TDMS)</td>
<td>331, 333</td>
</tr>
<tr>
<td>components</td>
<td>335</td>
</tr>
<tr>
<td>data protection</td>
<td>347</td>
</tr>
<tr>
<td>functionality overview</td>
<td>335</td>
</tr>
<tr>
<td>parallel processes</td>
<td>341</td>
</tr>
<tr>
<td>process control</td>
<td>337</td>
</tr>
<tr>
<td>system landscape integration</td>
<td>346</td>
</tr>
<tr>
<td>usage</td>
<td>348</td>
</tr>
<tr>
<td>use cases</td>
<td>332</td>
</tr>
<tr>
<td>user interface</td>
<td>336</td>
</tr>
<tr>
<td>Scope of processing</td>
<td>401</td>
</tr>
<tr>
<td>Scoring values</td>
<td>399</td>
</tr>
<tr>
<td>Scrambling</td>
<td>332, 334, 344</td>
</tr>
<tr>
<td>cross-system</td>
<td>350</td>
</tr>
<tr>
<td>set up</td>
<td>348</td>
</tr>
<tr>
<td>Scrambling (Cont.)</td>
<td>345</td>
</tr>
<tr>
<td>types</td>
<td>328</td>
</tr>
<tr>
<td>Secure data storage</td>
<td>135</td>
</tr>
<tr>
<td>Security</td>
<td>47, 114</td>
</tr>
<tr>
<td>Security patches</td>
<td>50</td>
</tr>
<tr>
<td>Segregation of duties (SoD)</td>
<td>251, 320</td>
</tr>
<tr>
<td>Sensitive data</td>
<td>322</td>
</tr>
<tr>
<td>Sensitive information</td>
<td>88</td>
</tr>
<tr>
<td>Separation of clients</td>
<td>205</td>
</tr>
<tr>
<td>Sequence of deletion</td>
<td>218</td>
</tr>
<tr>
<td>Service user</td>
<td>240</td>
</tr>
<tr>
<td>Shipping costs</td>
<td>219</td>
</tr>
<tr>
<td>Simulation</td>
<td>233</td>
</tr>
<tr>
<td>Single Sign-On (SSO)</td>
<td>374</td>
</tr>
<tr>
<td>SOX compliance</td>
<td>121</td>
</tr>
<tr>
<td>Special categories</td>
<td>286</td>
</tr>
<tr>
<td>Standard users</td>
<td>411</td>
</tr>
<tr>
<td>Starting field</td>
<td>267</td>
</tr>
<tr>
<td>Statistical key figures</td>
<td>95</td>
</tr>
<tr>
<td>Storage control</td>
<td>389</td>
</tr>
<tr>
<td>Storage limitations</td>
<td>32, 366</td>
</tr>
<tr>
<td>blocking and deleting</td>
<td>368</td>
</tr>
<tr>
<td>Subtypes controls</td>
<td>154</td>
</tr>
<tr>
<td>System architecture</td>
<td>339</td>
</tr>
<tr>
<td>System keys</td>
<td>350</td>
</tr>
<tr>
<td>System separation</td>
<td>198, 199</td>
</tr>
<tr>
<td>System states</td>
<td>259</td>
</tr>
<tr>
<td>System user</td>
<td>240</td>
</tr>
<tr>
<td>T</td>
<td></td>
</tr>
<tr>
<td>Table clusters</td>
<td>265, 277</td>
</tr>
<tr>
<td>Table hierarchy</td>
<td>263, 270</td>
</tr>
<tr>
<td>Table logging</td>
<td>122, 372</td>
</tr>
<tr>
<td>Target client</td>
<td>339</td>
</tr>
<tr>
<td>Target groups</td>
<td>108</td>
</tr>
<tr>
<td>Technical and organizational measures (TOMs)</td>
<td>60, 360</td>
</tr>
<tr>
<td>Technical controls</td>
<td>378</td>
</tr>
<tr>
<td>Technical measures</td>
<td>112, 127</td>
</tr>
<tr>
<td>Technical security</td>
<td>112, 124, 125</td>
</tr>
<tr>
<td>Test clients</td>
<td>332, 333</td>
</tr>
<tr>
<td>Third-party</td>
<td>29</td>
</tr>
<tr>
<td>Time constraint</td>
<td>101</td>
</tr>
<tr>
<td>Time limits</td>
<td>113</td>
</tr>
<tr>
<td>Time offsets</td>
<td>128, 229</td>
</tr>
<tr>
<td>Time reference</td>
<td>228</td>
</tr>
<tr>
<td>Time-based blocking</td>
<td>193</td>
</tr>
<tr>
<td>Trade union membership</td>
<td>34</td>
</tr>
<tr>
<td>Training clients</td>
<td>333</td>
</tr>
<tr>
<td>Transaction</td>
<td>299</td>
</tr>
<tr>
<td>ABOJ</td>
<td>260, 261</td>
</tr>
<tr>
<td>BP</td>
<td>293, 302, 308, 311</td>
</tr>
<tr>
<td>BUP_REQ_UNBLK</td>
<td>178, 180</td>
</tr>
<tr>
<td>CVP_DISPLAY_LOG</td>
<td>395</td>
</tr>
<tr>
<td>CVP_PRE_EOP</td>
<td>169, 171, 172</td>
</tr>
<tr>
<td>CVP_UNBLOCK_MD</td>
<td>179</td>
</tr>
<tr>
<td>DBIS</td>
<td>220, 261</td>
</tr>
<tr>
<td>DTINFO_ADRUST_MODEL</td>
<td>261, 264, 268, 278, 283</td>
</tr>
<tr>
<td>DTINFO_MODELING</td>
<td>264</td>
</tr>
<tr>
<td>DTINFO_PROCTRL_COLL</td>
<td>280</td>
</tr>
<tr>
<td>DTINFO_START_COLL</td>
<td>279</td>
</tr>
<tr>
<td>DTINFO_TEST_MODEL</td>
<td>269, 276, 279, 281</td>
</tr>
<tr>
<td>FB01</td>
<td>171</td>
</tr>
<tr>
<td>FB03</td>
<td>175, 184</td>
</tr>
<tr>
<td>FBLSN</td>
<td>177</td>
</tr>
<tr>
<td>FK01</td>
<td>185</td>
</tr>
<tr>
<td>ILM_DESTRUCTION</td>
<td>185, 236, 398</td>
</tr>
<tr>
<td>ILM_LIM</td>
<td>191</td>
</tr>
<tr>
<td>ILM_ARA</td>
<td>150, 229, 234</td>
</tr>
<tr>
<td>IRM_CUST_CSS</td>
<td>162, 235</td>
</tr>
<tr>
<td>IRMPOL</td>
<td>149, 151, 158, 160, 163, 166, 235, 237, 394</td>
</tr>
<tr>
<td>IRMRULE</td>
<td>230, 231, 237</td>
</tr>
<tr>
<td>IRMRULE_ACTIVATE</td>
<td>233</td>
</tr>
<tr>
<td>MEINJ</td>
<td>243</td>
</tr>
<tr>
<td>MK01</td>
<td>85</td>
</tr>
<tr>
<td>OBR8</td>
<td>220</td>
</tr>
<tr>
<td>OM89</td>
<td>219</td>
</tr>
<tr>
<td>PA30</td>
<td>100</td>
</tr>
<tr>
<td>PFCG</td>
<td>191, 398</td>
</tr>
<tr>
<td>RPMPOL</td>
<td>168</td>
</tr>
<tr>
<td>RSUSRZOO</td>
<td>406</td>
</tr>
<tr>
<td>RZII</td>
<td>403</td>
</tr>
<tr>
<td>S_ALR_78012177</td>
<td>92</td>
</tr>
<tr>
<td>S_ALR_78013611</td>
<td>94</td>
</tr>
<tr>
<td>SAGB</td>
<td>266</td>
</tr>
<tr>
<td>SARA</td>
<td>185, 218, 236</td>
</tr>
</tbody>
</table>
Transaction (Cont.)
SARI .................................................. 386, 393
SCASE .................................................. 192
SEO6 ...................................................... 402
SEII ...................................................... 266
SE16 ..................................................... 267, 386, 396
SE18 ...................................................... 284
SE19 ...................................................... 395
SM27 ...................................................... 401
SPRO ..................................................... 143, 149, 162, 257
SRALMANAGER ........ 289, 290, 292, 293, 295, 297
SRALMANAGER ......... 289, 290, 292, 293, 295, 297
SU21 ..................................................... 243, 259, 288
TDMS ..................................................... 336
VA03 ..................................................... 211
VF03 ..................................................... 213
VL03N ................................................... 182, 212
VORA ................................................... 220, 230
VORI ................................................... 219
VORJ ................................................... 220
XDO1 ................................................... 168
XDO2 ................................................... 173
XDO3 ................................................... 173
XX01 ................................................... 85

Transactional data ...... 83, 106, 140, 340
blocking ..................... 149, 181
Transport control .......... 389
Transport ................................. 400
Transport control .......... 390
Transport Management System .............................. 371, 403
Transport requests .......... 251

U
UI channels ......................... 292
Unblocking ......................... 179
request ......................... 178
Unified Connectivity solution .............................. 124
User activity ......................... 303
User administration .......... 412
User concept ......................... 409
User control ......................... 62
User data ......................... 92
Users ......................... 239

V
Validation mechanisms .......... 319
Vendors ......................... 85
master tables ................. 87
Vulnerabilities ................. 370

W
Web Dynpro ......................... 288, 291, 296
Where-used list ..................... 384
Volker Lehnert has held various positions in compliance and security at SAP since 2000. Since 2012, he has worked in SAP Application Innovation Services (AIS) as the product owner of data protection solutions, defining the data protection functions of the SAP Business Suite and SAP S/4HANA.

Iwona Luther has been working for SAP for 20 years in the field of data archiving, which has evolved over the years to SAP Information Lifecycle Management. She is the product owner of SAP ILM. She is responsible for data archiving courses through SAP Education.

Björn Christoph has been working for SAP as a software architect since 2002. He has been focusing for several years on topics such as data protection and software security in the SAP software.

Carsten Pluder has been working for SAP in support and development since 1999. He currently works for SAP Application Innovation Services (AIS) as lead architect for data protection for the SAP Business Suite and SAP S/4HANA. He focuses on supporting SAP customers in the archiving of their data and using SAP ILM.

Nicole Fernandes has worked as a translator for English, French, and German since 2005. Her fields of expertise are software/information technology and medical research/genetics. Her projects have included the translation of specialized ERP systems and industry-specific software solutions for the temporary employment sector.

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.