

Guideline Data Protection and Privacy for SAP - R/3

Release 4.6
Date September 28, 2001



SAP® AG • Neurottstr. 16 • D-69190 Walldorf
SAP reserves the right to amend this document.

Preface

This manuscript is a draft out of the guideline Data Protection and Privacy for SAP-R/3.

This guideline is addressed to Data Protection officials dealing with the German Applicants of SAP R/3. It contains recommendations not duties and obligations. Therefore, the controller and his data protection official remain solely liable for the appropriate implementation of Data Protection Law.

The topics are the requirements of the Federal Data Protection Act in Germany. The guideline contains 6 chapters, which deal with the German Applications of SAP R/3 Software:

1. The introduction process
2. Tasks of the data protection officials
3. The implementation of the rights for the persons concerned
4. The technical and organizational measures according to section 9 of the German Federal Data Protection Act (BDSG)
5. Commission on data collection and processing
6. Special themes like audit tools

The text at hand is the translation of chapter 4 of this guideline.

It mainly addresses the measures of security, which have to be fulfilled. Further requirements can be extracted from the framework of existing legislation in the English version of the Federal Data Protection Act (see http://www.bfd.bund.de/information/bdsg_eng.pdf) resp. the more general the English version of the European Union laws on data protection.

The guideline is authored by the data protection officials and examiners of German companies (see page 7 of the guideline) with support of SAP. The authors of this particular part, relating to the technical and organizational measures are:

Thomas Barthel FORBIT/CArO Hamburg

Georg Hohnhorst KPMG Deutsche Treuhand-Gesellschaft, Düsseldorf and

Thomas Glauch KPMG Deutsche Treuhand-Gesellschaft, Düsseldorf.

The guideline completes the security guidelines of SAP (www.sap.com/security) as well as the audit guidelines SAP R/3 FI (www.sap.de/revis).

The security guideline explains the basic mechanisms, which are examined in the data protection guideline and the audit guideline FI under the aspects legality and transparency.

If you have any further information or suggestions about the topics of the guideline please send a fax to the group representative of the working group on the enclosed form.

Preface.....	2
4. Implementing the Requirements of Article 9 of the German Federal Data Protection Act and its Appendix: Technical and Organizational Measures.....	6
4.1 Requirements	6
4.1.1 Statutory Requirements Resulting from Article 9 of the German Federal Data Protection Act.....	6
4.1.2 SAP Functionality for Meeting the Statutory Requirements	7
4.2 SAP Facts, Risks, and Measures.....	9
4.2.1 Identification and Authentication	9
4.2.2 Standard Users	11
4.2.3 User Authorization Concept: Selected Authorization Objects	13
4.2.4 User Authorization Concept: Selected Profiles	18
4.2.5 Special Features of the Authorization Check.....	20
4.2.6 User Administration.....	22
4.2.7 Changes to the Production System	23
4.2.8 System Interfaces	26
4.2.9 Auditing and Logging	28
4.2.10 Complex Search Help	30
4.2.11 Summary of the Key Risks	31
4.3 Summary of the Check Procedures.....	32
4.3.1 Checking Requirements	33
4.3.2 Checking Special Regulations from Priority Legal Specifications (for Example, from Valid Company Agreements on Organizational and Technical Measures)	40
4.3.3 Checking the Data Protection Measures in Accordance with Article 9 of the German Federal Data Protection Act and the Appendix	41
Index	50

4. Implementing the Requirements of Article 9 of the German Federal Data Protection Act and its Appendix: Technical and Organizational Measures

4.1 Requirements

This section deals with the technical and organizational requirements involved in processing and checking personal data. All the requirements must be met, that is, in particular with regard to processing outside the scope of national legislation.

These regulations apply to both production systems and upstream systems, provided that personal data can be accessed in these systems, or preliminary settings can be defined that are subsequently transported into the production environment.

The necessary technical and organizational measures have been extended on the basis of the EU Guideline 95/46/EG to both offer protection against accidental or unlawful destruction and accidental loss of data (Item 7: Availability Control) and to guarantee that processing is restricted (Item 8).

4.1.1 Statutory Requirements Resulting from Article 9 of the German Federal Data Protection Act

The German Federal Data Protection Act and, in comparable form, the German State Data Protection Acts, demand that the department responsible take technical and organizational measures to ensure that the requirements laid down in the Data Protection Act can be met. Measures must in particular be taken for compliance with the eight requirements listed in the appendix to the German Federal Data Protection Act.

Within the scope of SAP's implementation project, coordinated, suitable, and necessary measures must be identified and implemented at technical and organizational levels for the requirements listed in the appendix. This involves carrying out project-related risk analyses and implementing measures that apply at both organizational and technical levels. These measures are intended to prevent the unlawful and inappropriate processing of personal data and – where necessary/possible – to enable any cases of misuse to be detected. The relevant project steps, which should form the basis of the preliminary checks, are referred to in Section 1.

The technical and organizational measures should be coordinated to ensure that technical measures are effective, since these are supported by the presence of corresponding organizational measures. An example of this is a failure to implement the organizational features of the R/3 authorization concept, which, despite wide-ranging protection options, does not offer any protection due to the fact that many users have been assigned comprehensive authorizations. Diverse organizational measures lacking in technical support can be just as ineffective. Examples of this include

attempts in vain to ensure earmarking if an outflow of personal data from R/3 by means of the download function is not technically prevented.

4.1.2 SAP Functionality for Meeting the Statutory Requirements

The following table lists in the left-hand column the eight requirements resulting from the appendix to Article 9 of the German Federal Data Protection Act. The middle column provides selected starting points for implementing the requirements in the R/3 System. The right-hand column lists references to additional literature on this topic.

The objectives of the statutory requirements:	Starting points for the SAP R/3 System	Additional references
In accordance with the appendix to Article 9 of the German Federal Data Protection Act, 1.) Unauthorized persons must be denied access to data processing systems that process and use personal data (Access control)	Not relevant and, therefore, not supported by SAP Software	
2.) The use of data processing systems by unauthorized persons must be prevented (Access control)	Personal logon procedure (problematic when several users are using one device; additional resources (such as chip cards and PC security systems) must ensure that the users are able to switch between their logons without any problems; Auto logoff after a prescribed time limit; screensaver with password protection; Additional Single Sign-On and connection options for chip cards	SAP R/3 Security guide SAP R/3 Security Guide SAP R/3 Security Guide
3.) It must be ensured that persons authorized to use a data processing system can gain access only to access the data they are authorized to access and that personal data cannot be read, copied, modified, or removed without authorization during processing, use, and after being recorded (Access control)	Within R/3: by means of an adapted authorization concept, in line with the requirements of SAP, the Revision Guide, and data protection; Outside the R/3 System: encryption in the network, restrictive assignment of authorizations to SAP files and tables at database and operating system level; Download; Problem with the ABAP List Viewer: unprotected copying of entire files possible.	System documentation BC manual, 'Authorizations Made Easy' guide http://www.saplabs.com/auth FI Audit Guide R/3 Security Guide SAP Note 28777
4.) During electronic transfer or during transport or storage on	Within R/3: using the authorization concept;	System documentation, 'Authorizations Made Easy', BC

<p>data carriers, it must be ensured that personal data cannot be read, copied, modified, or removed without authorization. Checks must also be performed to establish where data transfer equipment is provided for transferring personal data (Transfer control)</p>	<p>Outside the R/3 System: encryption in network (LAN/WAN) and on other data carriers;</p> <p>For more information on the download function and the XXL List Viewer, see Item 3. For connection to the Internet: the Firewall concept and SAP Router;</p> <p>Authorization settings; the required verification, pursuant to Article 10, paragraph 4 of the German Federal Data Protection Act, is not supported.</p>	<p>manual R/3 Security Guide</p> <p>System documentation, BC manual, R/3 Security Guide</p> <p>If applicable, random samples via the trace function</p>
<p>5.) Subsequent checks must be performed to establish whether and by whom personal data has been entered, modified, or removed in data processing systems. (Input control)</p>	<p>Implemented systematically in all modules, for all SAP Objects, and for all data with automatic entry of creator/modifier, date, and time; in addition to display transactions, some of the modules provide additional reports for displaying change documents;</p> <p>If applicable, configuration of the change documents to be written</p>	<p>System documentation, BC manual, and Security Guide</p> <p>Functions for displaying the change documents in each technical function</p> <p>Recommendations Security Guide</p>
<p>6.) It must be ensured that personal data processed in the order can only be processed in accordance with the instructions from the sold-to party (Order control)</p>	<p>No particular support provided</p>	<p>See Sections 5.2.2 and 5.2.6 of this Guide</p>
<p>7.) It must be ensured that personal data is protected against accidental destruction and loss (Availability control)</p>	<p>Regular data backup at database level;</p> <p>Data backup concept;</p> <p>Authorizations adapted to the tasks at hand;</p> <p>Logging the key data modifications;</p> <p>Appropriate user training</p>	<p>System documentation</p> <p>See the general recommendations regarding data protection in the Security Guide</p>
<p>8.) It must be ensured that the data ascertained can be processed separately for different purposes.</p>	<p>Implementation by means of separation</p> <ul style="list-style-type: none"> • Of the systems • Of the clients <p>Within a client by configuring the authorization concept accordingly, in particular with regard to displaying and evaluating the data</p>	<p>See the R/3 Revision Guide and documentation Security Guide recommendations</p>

4.2 SAP Facts, Risks, and Measures

4.2.1 Identification and Authentication

4.2.1.1 SAP Facts

An R/3 User must log on to the R/3 System via SAP Logon using a user ID and password before he can access the information and functions in this system. By entering this data, the user identifies himself to the R/3 System and the system checks whether the user is authorized to work with the system. As regards the password, the settings made in the start parameters apply, provided no other changes have been made in the concrete installation. These parameter values, which are set during installation, are provided for a test system and must be reset for the production system. Transactions **RZ10** (Administration of Instance Profiles) and **RZ11** (Maintain Profile Parameters) are available for administrating the parameters.

The parameters relevant for identifying the user are explained in the following. The recommendations that are also specified afford a basic level of protection and are based on empirical values. It must be noted that the parameter values can be defined quite differently in each company, depending on the company's security policy.

- Minimum length of password
The `LOGIN/MIN_PASSWORD_LNG` parameter determines the minimum number of characters the password must contain.
Recommended parameter value: "6" (the minimum length is 6 characters.)
- Expiration period for the password
The `LOGIN/PASSWORD_EXPIRATION_TIME` parameter determines the interval for changing the password for dialog logon and ITS services that use the flow logic.
Recommended parameter value: "90" or less (the user must change his password after a maximum of 90 days.)
- Illegal passwords
Apart from the settings already mentioned, passwords excluded from use (for example, trivial passwords or keyboard combinations) can be defined in the table **USR40**.
- Additional Logon Variants
Depending on the Release, there are additional logon variants in addition to the password-based logon, such as:
 - Certification logons via the browser and Web server
 - SAP logon ticket (for example, for using the SAP Workplace/Enterprise Portal)
 - NT domain logon (NTLM)
 - PAS (Pluggable Authentication Services)
- Ending the SAP Session

The LOGIN/FAILS_TO_SESSION_END parameter determines how many failed logon attempts are permitted before the SAP session is ended. If the session ends automatically, this is registered as a failed logon attempt.

Recommended parameter value: “3” (The session is ended after 3 failed attempts.)

- Possible Logon Attempts

The LOGIN/FAILS_TO_USER_LOCK parameter controls how many logon attempts are permitted before the user is locked.

Recommended parameter value: “5” (The user is locked after 5 logon attempts.)

- Unlocking at Midnight

If the LOGIN/FAILED_USER_AUTO_UNLOCK parameter value is set at “1”, users who have been locked due to incorrect logons are unlocked at midnight.

Recommended parameter value “0” (automatic unlocking does not take place at midnight.)

- Automatic Logoff when Inactive

The RDISP/GUI_AUTO_LOGOUT parameter controls how much time in seconds is permitted before the user is automatically logged off. When a user is automatically logged off, data that has not been saved is lost, which results in the risk of data loss in the event of a “forced” logoff.

Recommended parameter value: “0” (The R/3 System does not automatically logoff. Instead of the SAP automatic logoff with the risk of losing data, a password-protected screensaver should usually be activated after 15 minutes.)

In the same way as the procedure for logging on to the system is controlled by parameters, the authorization check in the R/3 System is based on profile parameter settings. The recommended settings listed in the following again afford a basic level of protection. The following key parameters must be mentioned here:

- Deactivating Authorization Checks

Authorization checks can be suppressed with the AUTH/NO_CHECK_IN_SOME_CASES parameter. The number of authorization checks proposed by SAP can be reduced by using transaction **SU24**. This presupposes that the parameter is set to “Y” for deactivating the authorization checks. The value must be set to “Y” if the profile generator is used.

Recommended parameter value: “N” or “Y” if the profile generator is used

(Authorization checks are not deactivated if the parameter value is set to “N”. If the parameter value setting is “Y”, regular checks should be performed to determine whether the authorization checks have been deactivated in order to maintain access protection. Table USOBX_C and the procedure described in Section 4.2.5.5 can be used for this purpose.

- Authorization Checks for RFC
The parameter AUTH/RFC_AUTHORITY_CHECK determines whether authorization checks are made against the authorization object S_RFC for Remote Function Calls (RFC).
Recommended parameter value: “1” (the authorization check for RFC is active.)
- Authorization Check for ABAP Statements
The AUTH/SYSTEM_ACCESS_CHECK_OFF parameter enables automatic authorization checks to be deactivated for specific ABAP statements. These statements are, for example, file operations, calls for kernel functions, or CPIC calls.
Recommended parameter value: “0” (The authorization check for ABAP statements is active.)

4.2.1.2 Risks and Measures to be Taken

The following measures are suitable for combating the risk of impermissible access to the R/3 System and for activating the basic security mechanisms of the authorization concept instruments provided in the R/3 System:

- Defining the target values for the profile parameters and “illegal” passwords on the basis of a company-specific security concept.
- Adjusting the values of the profile parameters (transactions **RZ10**, **RZ11**)
- Maintaining the “illegal” passwords table (table USR40)
- Regularly monitoring the parameter settings (RSPARAM report or with the Audit Information System)
- Regularly monitoring the “illegal passwords” table (transaction **SE16** (Data Browser) for table USR40)

In addition or alternatively, depending on the overall IT architecture in which an R/3 System is included, further external security products are recommended. Such products include SNC (Secure Network Communications) or X.509 Client Certificates when using Web frontends. For SNC, the cryptographic library is available for downloading from the security homepage (*security* alias on the Service Marketplace).

4.2.2 Standard Users

There are a total of four standard users in the R/3 System. The function of these users is described in the following. It is particularly important that these standard users be protected within the scope of the technical and organizational measures to be taken.

4.2.2.1 SAP*

The SAP* user is the initial user hard-coded by SAP and, therefore, has all rights for the installation phase. Following the initial logon (for initial password, see the R/3 Security Guide) in the SAP System, a new user (unique assignment by name) must be created with comprehensive authorizations. This user is responsible for further administration tasks.

Even if the SAP* user does not have to carry out other activities, SAP* must not be deleted, as otherwise, provided no other technical measures are taken, all other users will be able to log on as SAP* using the standard password. Each time SAP* logs on, the user obtains the particular system rights associated with this user master record.

Consequently, for security reasons, SAP recommends that you withdraw all authorizations, or that the authorizations be restricted to display functions. SAP* should also be assigned to the "SUPER" user group to prevent this user from being deleted inadvertently; that is, SAP* cannot be physically deleted. If someone deletes SAP* via **SU01**, for example, SAP* will no longer be displayed in the user list, but will continue to exist in the system.

If the above measures are not taken, a new logon can be prevented via the following parameters:

Login/no_automatic_user_sap* with value "1"

(Automatic SAP* user is deactivated)

4.2.2.2 SAPCPIC

The SAPCPIC user is set up as a standard SAP user. The user cannot log on for dialog processing, but permits some programs and function modules to be called up in the SAP R/3 System. The user is only required within the EarlyWatch Service for collecting performance data, starting external background programs, and returning values for the Computer Center Management System (CCMS).

As a protective measure, the user can be locked in addition to the standard password being changed. SAP Note 29276 should be observed when implementing these measures.

In general, CPIC users should have function-related roles/profiles, even they cannot log on for dialog processing.

4.2.2.3 DDIC

In addition to SAP*, the DDIC user is defined by SAP. The DDIC user is used to maintain the ABAP Dictionary and the software logistics. As a result, extensive system rights are also stored for this user, in addition to those defined in the user profiles.

When the system is installed, DDIC is only created in clients 000 and 001 (for the initial password, see the R/3 Security Guide). If necessary, the DDIC user must be created for other clients.

Since DDIC is a user with special rights and is generally difficult to assign to one person, the use of DDIC is also subject to particular requirements with regard to the traceability of the activities carried out.

From the point of view of data protection, the SAP_ALL profile is not allowed for the DDIC user. Function-related profiles/roles should be created in order to perform the necessary activities (such as starting and stopping system monitoring tasks). Moreover, organizational considerations must be implemented to enable personal use (clear responsibility).

4.2.2.4 EarlyWatch

The EARLYWATCH user is the dialog user for the EarlyWatch Service in client 066. This user is only required for the Performance Monitor.

In order to protect this user from unauthorized access, the initial password must be changed. Technical and organizational measures must also be taken here to ensure that only those functions are carried out that are intended for this user.

4.2.2.5 Risks and Measures to be Taken

Special technical and organizational measures must be taken in order to combat the risk of unauthorized access to the R/3 System. These measures ensure that unauthorized viewing and unintentional/intentional manipulation of data is prevented. This also applies to special users, in particular.

The following measures should be taken:

- Create function-related roles/profiles for the above-mentioned users
- Lock users who are not required in day-to-day activities, or who are not active
- Configure the system parameters (see, for example, preventing logon with the SAP* user) in order to prevent unauthorized logons
- Regularly monitor the activities of the above-mentioned users
- Establish/create procedures for handling special users to support the technical measures

4.2.3 User Authorization Concept: Selected Authorization Objects

Key authorization objects from the HR module and Basis will be dealt with in the following section. Complete documentation for authorization objects can be obtained in the profile generator (**PFCG**) by double-clicking the authorization object. In older systems, this documentation is only available for the individual authorization objects in transaction **SU03** or via the Audit Information System (transaction **SUIM**).

4.2.3.1 Object P_ORGIN

The authorization object P_ORGIN (HR: master data) is used as part of the authorization check for personal data (master and time data). A check is generally performed when HR infotypes have to be processed. The organizational assignment of the HR master data, the data view (infotypes), and the authorization level are important here.

The object consists of the following fields:

AUTHC	Authorization level
INFTY	Infotype
SUBTY	Subtype
PERSA	Personnel area
PERSG	Employee group
PERSK	Employee subgroup

VDSK1 Organizational key

In the “Authorization level” field, it must be noted that other objects (such as *HR: Applicants* or *FI: Travel planning*) are used for test purposes (see the SAP Object documentation for further details).

The following values are also important with regard to the authorization level (see the SAP Object documentation for further details):

R	Read
W	Write
M	Matchcode (recommendation: you should never assign just W or just R, otherwise the users will not obtain any search help (previous matchcode search) and must always directly enter the personnel number.)
S	Writing locked, unlock, provided the last person to change the record was not the current user.
E	Writing locked
D	Change the lock indicator

In addition to the authorization object P_ORGIN, an authorization is required for maintaining the master data for the relevant transaction, for example, **PA30** (Maintain HR Master Data).

4.2.3.2 Object P_ABAP

Two objects are provided in SAP for protecting access to reports. The first object is **S_PROGRAM** (ABAP: Program Flow Check, object class BC_C) and the second is the HR: Reporting object **P_ABAP**.

The S_PROGRAM object first controls whether and which reports can be accessed, provided the user is authorized to access the authorization group of the report (see Section 4.2.5.4 below). The P_ABAP object controls how the objects:

- HR: Master Data (P_ORGIN)
 - HR: Master Data – extended check – (P_ORGXX)
 - Structural authorization check in specific reports
- are used to check the authorizations for HR infotypes. By configuring the fields:
- REPID (Report name)
 - COARS (Degree of simplification for authorization check), accordingly, you can override infotype authorizations, that is, they can be removed from the check.

SAP created this object to enhance processing by “deactivating” additional authorization checks.

As a result, the attributes of this object must be examined critically to ensure that personal data cannot be displayed with the reporting function.

4.2.3.3 Object P_TCODE

The object P_TCODE is an application-specific authorization object and is a forerunner of the authorization object S_TCODE. The attributes of the object P_TCODE (HR: Transaction Code) enable access to various HR

transactions to be protected. Note that this object is not used for all HR transactions, which means that the object S_TCODE must also be used.

The tables USOBT and USOBX can be used to determine which transactions are protected by the attributes of the object P_TCODE. These tables are evaluated for the object by entering “P_TCODE” in transaction **SE16**.

4.2.3.4 Object S_TCODE

When transactions are called up, the object **S_TCODE** checks whether the user is authorized to execute the selected function. The Transaction code (TCD) field is defined for this object.

Configuring this object for specific functions enables access protection measures to be mapped at an initial level. Provided that no further settings are defined for this object, the module or function-specific objects are used in the remaining authorization checks.

All of the objects that correspond with one another must be configured accordingly to ensure that the requirements of the German Federal Data Protection Act are sufficiently covered.

4.2.3.5 Table TSTCA

All the transactions with additional check objects are stored in table TSTCA. The table can be evaluated using transaction **SE16**.

This table must be maintained in line with the CTS and CTO (Change Transport System and Change Transport Organizer) mechanisms, since it contains cross-client entries.

Note that access authorization checks can be bypassed by deactivating the authorization checks (by removing the check object) – using application development functions (ABAP programming).

4.2.3.6 Converting Reports to Transactions

SAP provides two options for assigning reports to transactions. The first is automatically carried out when the report is integrated in an area menu or in a role menu. There is, however, no obvious connection between the report and the transaction name, as SAP numbers the transactions consecutively (structure S_XXX_XXXXXXXX). For this reason, the second method is preferable: Reports are stored with a transaction set by the user and are started by calling up this transaction. With both methods, note that the user can also start the reports via the “normal” reporting function if he has authorization to use transactions such as **SA38** or **SE38**. Reports can also be started indirectly from **SE80** and **SE84**, and various other transactions.

From the point of view of the Data Protection Act:

a) A concept for protecting the individual reports must be elaborated (authorization concept S_PROGRAM, administration report RSCSAUTH) and

b) An analysis must be performed to determine whether, and to what extent, the authorization checks can be circumvented, if necessary, using the methods described.

4.2.3.7 Object S_TABU_DIS and S_TABU_CLI

The object **S_TABU_DIS** controls the access to the table maintenance functions (using standard tools such as SE16, SM30, and so on). The object **S_TABU_CLI** controls the access to the cross-client table maintenance functions. In addition to the appropriate settings for these objects, transaction authorizations are required for maintaining tables (see S_TCODE).

The object **S_TABU_DIS** consists of the *Activity* and *Authorization group* fields. The type of access to tables (display or change) can be controlled by setting the *Activity* field accordingly. The *Authorization group* field is used to restrict access to certain tables.

The object **S_TABU_CLI** consists of the *Indicator for cross-client maintenance* field.

From the point of view of the Data Protection Act, access to the authorization groups for these tables (for example, the infotypes in the PA table) should be restricted to prevent unauthorized access to personal data with transaction **SE16**.

Authorization groups can be assigned to tables by calling up the transaction **SE16** and specifying the table V_DDAT.

4.2.3.8 Object S_TOOLS_EX

Authorizations can be assigned via the object S_TOOLS_EX (object class BC_A). These authorizations are used to display external statistics records for using monitoring tools.

This object contains a field (AUTH), via which authorization names can be assigned. The entry S_TOOLS_EX_A allows access to external statistics.

To prevent service and behavior checks from being performed, this access should only be restricted accordingly. User behavior may only be evaluated in justified and agreed exceptional cases.

Particular attention must be paid to the co-determination rights of the employee representation board when this authorization is assigned.

4.2.3.9 Object S_SCD0

The authorization object S_SCD0 (change documents, object class BC_Z) provides access to change documents and change document objects. Change documents are created for modifications to master data and user master records, for example.

Change documents (master data) form part of documents (long-term documents) that must be kept pursuant to Article 257 of the German Commercial Code. Change documents and change objects can be maintained (=changed) or deleted in SAP by appropriately configuring the object S_SCD0 (see User authorization concept), and, therefore, can directly influence the logging function.

Particular attention must be paid to the co-determination rights of the employee representation board when this authorization is assigned.

4.2.3.10 Objects for User and Authorization Maintenance (S_USER_xxx)

The six different authorization objects for user and authorization maintenance (see Section 4.2.6.1) enable the processes for creating and maintaining users and assigning users authorizations to be tailored to the company's needs.

As far as data protection legislation is concerned, these processes must be carefully configured so that access is reserved for authorized persons only.

4.2.3.11 Object S_GUI and XXL List Viewer

SAP offers the option of transferring various evaluations by download or by using the XXL List Viewer from the "secure SAP Environment" to the PC and further processing them without any additional checks. All data that is displayed on the screen on the basis of the authorizations assigned to the user can also be transferred to the PC. The XXL List Viewer functions can currently only be protected to a limited extent by the object **S_OLE_CALL**.

SAP provides the object **S_GUI** to protect the download function. The "Activity" field is currently defined for this object. The only possible value is "61". This value authorizes the user to save all the lists that can be displayed on the screen as local files. Additional authorization checks (for started reports and transactions, for example) can be added via a user exit (see SAP Note 28777).

4.2.3.12 Object S_SPO_DEV

Authorizations can be assigned for printing on the specified printers via the object **S_SPO_DEV**. By generically assigning printer names, for example, you can specify that users of the HR module can only print on printers in the HR department.

4.2.3.13 Risks and Measures to be Taken

To prevent the risk of unauthorized access to personal datasets, the above objects must be configured in such a way that only the data relevant for the work center in question can be read and maintained.

If HR is used, the user authorization object, therefore, must be configured in such a way that access to the above objects and to all other objects in the Human Resources class is restricted and separated by the function. Access to all infotypes should also be severely restricted.

In particular it must be ensured that:

- Technical and organizational measures are put in place that deny the access required for changing and deleting change documents. Access via reports, such as RSCDOC99, must be prevented in particular.
- Data can only be downloaded as authorized, that is, it must be ensured that the authorization concept is adequately configured so that only function-based data access is possible
- Misuse of the data by the download function and/or the XXL List Viewer is prohibited and that subsequent processing for purposes not

permitted by the Data Protection Act or for impermissible reasons (such as inadequate checkability) is excluded

- Table display and maintenance authorizations are adequately restricted by the configuration of the authorization class field
- Access, in terms of the options for changing transactions and programs, is handled in an extremely restrictive manner, or that access is prevented by means of organizational rules (including the creation of organizational instructions regarding the procedure documentation for the maintenance measures to be taken)
- As a rule, change documents cannot be deleted in the production system (with the exception of emergency users), or only by the archiving and reorganization programs provided
- The authorization level field is defined restrictively with regard to access to HR infotypes
- The objects P_TCODE and S_TCODE are appropriately configured

If, on the basis of the available workforce, it is not possible to configure the above objects in a complex manner and on a function basis, it is recommended that the organizational instructions stipulate the use of downstream checks. A neutral department must check compliance with these instructions at regular intervals.

4.2.4 User Authorization Concept: Selected Profiles

System administrators must be set up in order to be able to carry out the necessary system administration tasks. These system administrators naturally have extensive authorizations. For this reason, SAP generally provides the following delivery profiles in the standard system for use in the test system. These delivery profiles must, however, be adapted in line with the requirements of the company.

In the event of an emergency, or in the event of an upgrade or release upgrade, comprehensive rights (authorizations or profiles) may have to be assigned temporarily. Note that a different person assigns these rights (double verification principle) and that it is ensured that these users and authorizations are deactivated outside the required usage time.

4.2.4.1 SAP_ALL Profile

This profile grants practically unrestricted access to the entire system (including applications), including, above all, access to application development tools. Using the various authorizations contained in this profile, therefore, can endanger data storage and data processing in line with the German Federal Data Protection Act in the same way as the adequacy of the accounting data.

4.2.4.2 SAP_NEW Profile

The SAP_NEW profile provides authorizations for new authorization objects for existing functions. The individual fields of the objects contained in the SAP_NEW profile are generally set to comprehensive values (*). SAP_NEW is shipped on a release-specific basis.

Since the object configurations contained in SAP_NEW, in connection with the authorization concept implemented in the company, leads to unwanted authorization enhancements, this profile should not be assigned to any user in a productive SAP System.

4.2.4.3 P_BAS_ALL Profile

SAP also ships standard profiles for the HR area in test systems. The P_BAS_ALL profile (all authorizations for personnel data) enables comprehensive access to personal data. Furthermore, the contents of other applications can also be displayed by the general table display functions. This profile should not be used in production systems.

4.2.4.4 Other S_xxx Profiles

The profiles described in the following are simply models. In general, the settings for the individual objects in these profiles must be restricted on a function basis.

S_A.SYSTEM This profile is provided for the central system administrator for assigning all the Basis authorizations (without modules). This profile also contains the authorizations for user administration.

S_A.ADMIN This profile is provided for the system operator and contains the authorizations for application development, for administrating the SUPER user group, and for maintaining the S:A group profiles.

S_A.CUSTOMIZ This profile contains the authorizations for making Customizing settings.

S_A.DEVELOP This profile is provided for application developers with the relevant programming authorizations.

4.2.4.5 Risks and Measures to be Taken

To combat the risk of unauthorized access to the R/3 System and to activate the basic protection mechanisms of the authorization concept instruments provided in the R/3 System, the profiles listed above should not be assigned in a production system. This is above all necessary when:

- Checking or traceability is not provided by the use of the replace function when debugging or deleting change documents (part of the authorizations in SAP_ALL)
- The data protection requirements are violated due to a failure to adapt the authorization concept
- Access protection for the R/3 System is circumvented by means of the programming means (in particular, circumvention of the authority check)
- The system status is changed, for example:
 - Access authorizations are assigned to an unauthorized user or for impermissible programs
 - Files, data fields, or keys that have not been agreed upon are configured

- Infringements are concealed by changing the system parameters, for example by:
 - Falsifying the log files, for example by temporarily deactivating table logging. This, however, requires access to the profile parameters, the table activation authorization, or the developer authorization
 - Circumventing access authorization checks by deactivating the authorization check

The “model profiles” shipped by SAP must generally be adapted in terms of their functions to the requirements of the company to ensure adequate access protection that meets the various statutory requirements.

The exception to this requirement is permission to assign the SAP_ALL profile to emergency users, whose activities are suitable for logging, for example using the Security Audit Log (SM19/SM20).

4.2.5 Special Features of the Authorization Check

4.2.5.1 Deactivating Authorization Checks

As described in Section 4.2.1 (Identification and Authentication), authorization checks can be deactivated in the R/3 System either for specific transactions or globally (transactions **SU25** and **SU26**) (the exception to this are the HR and BC modules.).

4.2.5.2 Authority Check for Programs (Own and SAP)

Access protection in R/3 Systems is essentially based on automatic checks stored in the in programs. This involves the ABAP “Authority Check” statement, which can be stored in the coding of the programs. When a program is run, the authority check checks whether the authorizations of the user who is calling up the program are adequate. If so, access is granted to the information; if not, the program must be configured in such a way that access is denied.

Reliable access protection can only be ensured if the authority checks are stored correctly in the coding of the programs. This applies to both standard R/3 programs and customer-specific reports.

4.2.5.3 HR Program Switch (Table T77S0)

As described, the authorization object P_ORGIN (HR: master data) has a particular significance regarding access to personal information. Whether this authorization object and other HR authorization objects or structural authorizations (switch PLOGI AUTH ORGPD) are tested by the system depends on the Customizing settings. In Release 4.6B, storage takes place in table T77S0 (system table). In this table, semantic codes determine whether the authorization objects are active for authorization checks. In Release 4.5 and earlier releases, similar control data is managed in the program MPPAUTSW (customer include with switches for the authorization check).

There is currently no systematic method for checking the assigned structural authorizations with the user information system. The check,

therefore, must be performed for each individual authorization.

4.2.5.4 Report Authorization Groups

Access to sensitive reports can be protected by means of transaction code assignment or authorization groups in addition to the authority checks mentioned above. If the transaction code assignment method is used, it must be ensured that user reports can only be called up via a specifically assigned transaction. In this case, it must not be possible to call up reports via transactions such as **SA38** (ABAP reporting).

Alternatively, protection may be implemented via authorization groups. Each relevant report should be assigned to a specific authorization group. Reports that are not used should be assigned to a 'locked' authorization group, and generally accessible reports to a 'general' authorization group. Assignments can be made with report RSCSAUTH. Accordingly, the authorizations for the object S_PROGRAM (ABAP: Program Flow Checks) must be defined in the authorization concept.

4.2.5.5 Risks and Measures to be Taken

Deactivating authorization checks can be extremely risky, since this can disable the access protection mechanisms provided in the standard R/3 System. In addition to checking the parameter AUTH/NO_CHECK_IN_SOME_CASES, the following procedures can be used for monitoring purposes:

- Display table USOBX_C (check table for table USOBT_C) using transaction **SE16** (Data Browser)
- Analyze whether the table contains entries with OKFLAG = N. The authorization check for the relevant authorization objects is deactivated for specific transactions

As far as authority checks are concerned, the following measures form suitable starting points for ensuring data protection:

- Create development guidelines for programming customer-specific ABAPs. These guidelines must stipulate, for example, how authority checks are performed, the authorization groups for reports, as well as test, release, and documentation requirements.
- Refer to the relevant SAP Notes (SAP Service System) for the standard R/3 programs so that the authority checks can be extended or corrected in the programs if corrections need to be made.

With regard to the HR program switch, the settings for the active HR authorization objects must be determined as target values. The actual settings made in the R/3 System (table T77S0 or program MPPAUTSW) should be monitored at regular intervals. Furthermore, measures must be defined that prevent unauthorized users from maintaining the program switch.

With regard to the report authorization groups, the authorization concept should define which measures must be taken to protect reports from unauthorized access. If authorization groups are used for this purpose, the assignments of reports to authorization groups should be monitored periodically. When a release is upgraded, note that new standard R/3

programs have to be included in authorization groups.

4.2.6 User Administration

4.2.6.1 Central User Administration Concept

As described, the R/3 user is identified in the system by means of his or her user master record. The user's access rights are stored in the user master record. For storing this data and for maintaining the access rights in the user master record, the R/3 System offers various organizational alternatives that are described in the following.

In the case of central user maintenance, a central department is responsible for maintaining all the user master records. Roles and profiles can be assigned either centrally or locally (settings can be made via Customizing or at object or field level).

Since user administration and the administration of access rights represent activities that are problematic for security, the R/3 System offers the option of mapping a principle of multiple verification.

SAP, therefore, recommends that a **user administrator**, a **role administrator**, and an **activation administrator** be created to ensure functions are separated.

The user administrator's tasks involve creating and maintaining user master records.

The role administrator maintains the authorization concept elements. Depending on the authorization concept, these elements are either roles, profiles, or authorizations.

The activation administrator is responsible for the usability authorization concept elements. The tasks involved here also depend on the authorization concept and include activating authorizations and profiles created by the role administrator in the maintenance version. They can also involve comparing users. In this case, the roles containing the stored profiles and authorizations are assigned to the user master records.

SAP has defined the following authorization objects in the "Basis Administration" object class in order to enable the different administration tasks to be separated:

- User master maintenance: User groups (S_USER_GRP)
- User master maintenance: Authorizations (S_USER_AUT)
- User master maintenance: Authorization profile (S_USER_PRO)
- Authorization system: Check for roles (S_USER_AGR)
- Authorization system: Transactions in roles (S_USER_TCD)
- Authorization system: Field values in roles (S_USER_VAL)

4.2.6.2 Local User Administration Concept

With this form of administration, maintenance tasks can be distributed to several departments. The user group can be used to control which user master record an administrator is responsible for. Organizational responsibilities can be mapped in the system using corresponding

authorizations for the authorization object S_USER_GRP (User master maintenance: User groups).

4.2.6.3 Conventional User Administration with Profiles

In addition to the difference between central and local user maintenance, a distinction must also be made as to how a user obtains his access rights. In the case of conventional user administration, these rights are assigned directly via profiles (single or composite profiles) in the user master record. When the user administrator maintains a user master record, the changes take effect as soon as the user logs on to the R/3 System.

4.2.6.4 User Administration Using the Profile Generator

In addition to profiles, access rights can also be stored in roles. Roles are stored in the user master record. Conversely, the user master records can be assigned to the roles.

Unlike conventional user maintenance, time-dependent role assignments can be defined (temporary assignment of authorizations). The reconciliation process can be started from user maintenance or role maintenance. The transaction **PFUD** (User Master Data Reconciliation) and the report RHAUTUPD_NEW (User Master Data Reconciliation) are also available.

4.2.6.5 Risks and Measures to be Taken

The risk associated with the user administration essentially entails unauthorized users accessing the R/3 System and unauthorized or too many access rights for the user master records that have been created. This risk must be combated by organizational measures, such as the multiple verification principle and technically mapping these measures in the R/3 System.

The authorization objects described in Section 4.2.6.1 are provided for this purpose. These objects can be configured for the relevant administrators to provide a separation of functions as described above.

Since the division of functions is often not considered adequately with regard to the standard R/3 profiles and roles from a data protection perspective (see, for example, S_A.SYSTEM or SAP_BC_USER_ADMIN_AG), company-specific elements need to be created. The above objects must then be configured in accordance with the resulting requirements.

If, on the basis of the workforce available, it is not possible to divide functions into three levels (triple verification principle), it is recommended that the functions be divided into at least two levels (user administration with role assignment and authorization administration with role and activation administration).

4.2.7 Changes to the Production System

Changes that are made in the production system are subject to the procedure logging requirements that are implemented for verification purposes. These requirements result from Article 238 of the German Trade

Law ff.

To ensure that changes are logged, various system settings must be made or basic protection mechanisms must be activated that prevent unauthorized changes from the outset.

4.2.7.1 Change and Transport System

Definition

CTO

The Change and Transport Organizer (**CTO**) provides functions for creating, documenting, and releasing change requests in Customizing.

TMS

The TMS supports the organization and transportation of these requests.

As a rule, SAP recommends that three separate SAP Systems be used for application development and Customizing – a **development system**, a **quality assurance system** and a **production system**.

Consequently, due to

- Maintaining the dataset protection
- Protecting against unauthorized display of personal data
- Tracking changes to the system,

authorizations for application development and Customizing should not be granted in a productive SAP System. To configure the transport routes for the three systems above, administration authorizations are required (object S_CTS_ADMIN).

Changes should generally first be made in the development system and transported into the **quality assurance system** using the TMS.

Once an appropriate test, acceptance, and release procedure has been carried out, the settings are made in the production environment via the TMS.

Depending on the configuration and dataset, personal data protected by the Data Protection Act can occur in all systems.

The logs created for the TMS ensure that the settings are tracked.

Extensive logs for transports that have been performed and changes that have been made, and so on, can be accessed from transactions **STMS** and **SE03**.

4.2.7.2 Table Logging / Customizing

When SAP is implemented and while it is in operation, a large number of tables are adapted to the requirements of the company.

Since changes to tables can generally be treated as program changes, any changes that have been made since production startup must be logged. The table change logs must be kept for the statutory storage period (10 years).

By default, SAP does not provide for the table changes to be logged, due to the extensive Customizing settings required.

The **rec/client** parameter is set to **OFF** for the test system. This setting

must then be changed in the development system at the start of Customizing work and in the production system after production startup by changing the standard profile (DEFAULT.PFL) so that either all table changes in the system (**ALL**), or at least the table changes in the delivery client (**000**) and the productive client(s) are logged. The **ON** setting is not permitted.

When the **rec/client** parameter is activated, change log records are written for those tables where the relevant indicator is set in the technical settings. Customers must mark **tables (T9, X, Y, or Z)** they have created themselves to indicate that they require logging.

Table log indicators are maintained with transaction **SE13**.

In general, Customizing settings should not be made in the production system so that a test, acceptance, and release procedure must be carried out and to ensure that the settings that have been made are in line with the relevant requirements.

Note that when using the TMS, you must ensure that logging is also performed in the target system when Customizing changes are transported. In the configuration, the parameter **RECCLIENT** (parameter for table logging) must be set at the time of import (this parameter is not the same as the **rec/client** for table logging in the production system).

4.2.7.3 System Change Option

You can use transaction **SE06** to define whether repository objects and cross-client Customizing objects can be changed.

Individual objects, such as:

- Customer developments
 - SAP Basis components
 - Development Workbench,
- can be specifically protected. You can use a pushbutton assigned to this transaction to evaluate the relevant change logs.

The protection mechanisms established in this transaction do not affect the client-specific Customizing changes.

Appropriate protection mechanisms for these settings are configured by means of the client control settings (see Protecting table T000).

4.2.7.4 Logs

When changes are made to objects/tables in SAP, an entry is created in a change log file, provided the relevant system settings have been made. This file is stored in the SAP file/database system. Each SAP installation has its own database and, therefore, its own file/database system. Exceptions to this are transport logs, which are stored in a common transport directory.

4.2.7.5 Protecting Table T000

By defining the relevant settings for table T000, you can prevent changes from being made to the SAP System in general or in specific subareas. Transaction **SM30** is used to display and maintain the relevant settings.

Various settings can be made with regard to

- Changes for transports and client-specific objects
- Changes to cross-client objects
- Protection for client copy tools and reconciliation tools.

In general, the settings should be defined in such a way that changes cannot be made in the production system.

If it becomes necessary to open the system with regard to change options, it must be ensured that no unchecked changes are made (corresponding documentation should be created) and that the change status is reset once the settings have been made.

4.2.7.6 Risks and Measures to be Taken

To ensure proper use of the program and to protect against unauthorized display or unintentional/intentional manipulation of data, it must be ensured that the system settings provide adequate protection against changes and that the necessary change logs are created. In this respect, it should be ensured that

- Clear and binding regulations are met with regard to maintaining, checking, and logging tables in order to be able to meet the statutory requirements, and to prevent the risk of datasets being manipulated purposely or inadvertently, as well as to meet the requirements for protecting personal data
- The relevant system parameters are set with respect to the TMS, transaction SE06, and the settings for table T000
- The logs created can be kept in accordance with the statutory storage periods and that, if necessary, they can be made readable again.

Regular checks of the settings made and downstream checks of the change documents are also necessary.

4.2.8 System Interfaces

SAP provides various interface methods for communication within an R/3 System, for exchanging information between different R/3 Systems, and for communication between R/3 and non-SAP systems.

4.2.8.1 Batch Input

With the batch input method, data is saved in a batch input session. The data is then transferred by importing the batch input session. The batch input session simulates the online entry of transaction codes and data, and is subject to the relevant authorization and plausibility checks.

4.2.8.2 RFC, ALE, BAPI

Remote Function Calls (RFC) are used for communication between distributed programs in an R/3 System landscape. RFCs can be used to call up function modules in a non-SAP R/3 System and to return the results to the calling R/3 System.

RFC technology also forms the basis for other R/3-specific interface

methods, such as Application Link Enabling (ALE) and Business Application Program Interfaces (BAPI).

4.2.8.3 PC Download

SAP offers the option of transferring various evaluations by download from the “secure SAP environment” to the PC for further processing without any additional checks. The download function applies to the types of list outputs that can be transferred to the PC via the menu.

Menu path:

System -> List -> Save -> Local file

Various authorization objects are provided in the R/3 System for combating the risk of personal data being transferred and possibly misused during processing.

4.2.8.4 ABAP List Viewer

The ABAP List Viewer, which is installed in many programs, enables displayed data to be transferred into any other program using the copy and paste functions, without being subject to any further authorization check or logging.

4.2.8.5 Risks and Measures to be Taken

Following each data export in to non-SAP systems, earmarking, deletion periods, and other requirements of the Data Protection Act can no longer be ensured within the SAP environment.

For all types of interface processing, the main risks are

- Incomplete or incorrect processing
- Manipulation during data transfer or the program run
- Unauthorized viewing of personal data
- Uncontrolled transfer of this data.

Suitable measures must be taken to combat these risks. As far as organizational measures are concerned, all interface files and the procedure used should generally be documented in accordance with the requirements laid down in the German Federal Data Protection Act (Article 4g of the German Federal Data Protection Act, key word “Monitoring Proper Application” and Article 4e of the German Federal Data Protection Act, key word “Describing the Data or Data Categories”).

As far as technical measures are concerned, different internal check levels are provided in the R/3 System, for which settings must be defined correctly (in particular in terms of the interaction between checks) and regularly monitored. The key technical aspects include the following:

- With regard to the batch input procedure, the authorization concept can determine which users can create, process, and delete batch input sessions. Access is determined by authorizations for the authorization object S_BDC_MONI (batch input authorizations).
- With regard to Remote Function Call technology (RFC), note the RFC destination security settings (transaction **SM59** - RFC Destinations).

These settings are maintained by the authorization object S_ADMI_FCD (system authorizations). The setting for the profile parameter auth/rfc_authority_check specifies whether authorization checks have to be performed for the RFC. The parameter can be monitored by the report RSPARAM, for example. For security reasons, it is strongly recommended that the authorization check be activated for the RFC. If so, the access protection checks are performed using the authorization object S_RFC (authorization check for RFC access).

- With regard to Application Link Enabling (ALE), the distribution model and the ALE authorizations must be maintained. The SALE menu can be used to access the relevant functions. The transactions and reports contained in this menu must then be protected accordingly.
- With regard to the PC download, the authorization object S_GUI (authorization for GUI activities) is available for checking the generic download of lists. Personal data in the individual applications must be protected by application-specific authorization objects.
- With regard to the ABAP List Viewer, the relevant function modules can be removed from critical programs by making changes to the program.

4.2.9 Auditing and Logging

The configuration and evaluation of the following logs must be coordinated with the person responsible for data protection. Note that the co-determination rights of the employee representation board must also be observed.

4.2.9.1 Audit Information System

The Audit Information System (AIS) was developed by SAP to support auditors, internal revisers, system auditors, and persons responsible for data protection. The AIS provides a collection of reports relevant for auditing purposes that enable the above employee groups to carry out extensive evaluations without having any specific knowledge about the necessary reports.

The findings and requirements of the different working groups (revision group, data protection group) have been incorporated in the AIS functionality.

As of Release 3.1i, the AIS can be subsequently installed free of charge. Since Release 4.6, the AIS has been part of the standard system. Transaction **SECR** is used to start the AIS. The folder structure displayed provides access to

- Business audits
- System audits

Subareas of the system audit represent checklists in accordance with the R/3 Security Guide and checklists in accordance with the Data Protection Guidelines.

SAP plans to revise the AIS as of Release 4.6c. This will involve, among

other things, replacing transaction **SECR** with corresponding roles.

4.2.9.2 Security Audit Log

Since emergency users that have been set up are generally provided with the **SAP_ALL** profile, verification must be supplied of the activities carried out, in line with the statutory requirements.

To use the Security Audit Log, the appropriate parameter settings must be made.

Transaction **SM19** can be used to specify which events are to be logged for each instance, client, and user. Downloads can now also be logged. The possible settings must be taken from the SAP documentation.

Transaction **SM20** enables the logs created to be evaluated.

In order to create logs, the entry **RSAU/ENABLE** must be set to 1 in the profile parameters, in addition to the parameter settings above.

From a data protection perspective, it is recommended that the emergency users that have been set up with extensive rights are subject to compulsory logging and that the use of downloads is logged for all users. Events that represent a breach of security can be displayed as alerts on computer center consoles in the CCMS.

4.2.9.3 System Log

The SAP R/3 System generally logs different error situations in system logs (syslog at application level); these include:

- Logon attempts that lead to locking
- Processing terminations
- Other problems and warning messages

The syslog can be called up with transaction **SM21**.

Since the syslog is generally deleted at short intervals, it is only of limited use for checking for unusual system activities and any infringements of the various regulations, unless organizational instructions exist with regard to regular monitoring of the messages shown.

When you call up the syslog, you can use the search function to search for unusual activities or errors, in particular via the column Tcod (transaction code). From the point of view of the Data Protection Act, this particularly applies to transactions from the areas **PA** and **PD**.

4.2.9.4 Transaction Logging STAT (CCMS)

SAP offers the option of logging all on-going activities via the **CCMS** (Computing Center Management System) for specific transactions and users on the application server. Statistical data can be created for each user on a daily, weekly, or monthly basis. (Transaction **STAT** with **RSSTAT020** and **STAD** with **RSSTAT026**)

4.2.9.5 S_TOOLS_EX

The SAP objects **S_TOOLS_EX** with field **AUTH** value **S_TOOLS_EX_A** and **S_ADMI_FCD** with field **S_ADMI_FCD** value **STOR** are required for displaying statistical data on users. From a data

protection perspective, the use of this function and its assignment must be subjected to a critical examination. Monitoring particular events (such as workflow activities)

It must also be assumed that the workflow component (as part of the SAP Basis module) will be used more in the future. The workflow component provides tools for automatically controlling and processing application-specific processes. This enables all of the individual user's processing steps (execution time, duration, and so on) to be logged automatically (using SWU9, SWI2, SWI5, for example).

If the workflow component is used, evaluation options are provided with regard to user behavior (for example, the number of activities processed, and so on).

4.2.9.6 Report Logging in HR

Downstream checks for starting "critical reports" can be maintained in table T599R (V_T599R). Provided the settings made ensure that logs are created, an evaluation can be carried out using report RPUPROTD.

From a data protection perspective, it is recommended that the use of flexible evaluations (such as reports RPLIC010 and RPLMIT00) and flexible absence evaluations (the RPTABSxx reports) be logged at least.

4.2.9.7 Risks and the Measures to be Taken

For the issues described above, a distinction must be made between evaluations that enable downstream checks in the sense of the internal check system (IKS) and those that facilitate activity-related checks and, therefore, service and behavior checks.

If the workflow component, and to a lesser extent the syslog or the CCMS (STAT) is used, evaluation options are available with regard to user behavior (for example, the number of activities processed, and so on). The use of these evaluations can be specifically restricted via the authorization concept. In relation to this, it is necessary to check the authorizations defined in the particular company. The AIS offers a good starting point for this check.

We regard the use of the security audit log to trace the activities of specially created emergency users as essential. This log represents an active component of a comprehensive security management concept. In this respect, it is important that a basic organizational framework be created above and beyond the technical measures described. This framework must ensure that the passwords of emergency users can be administered and reset, and the logs that have been created can be archived and checked.

4.2.10 Complex Search Help

SAP has extended the search help function in the last releases. In many modules, such as the HR module, these functions represent separate information systems. The available search help functions can be restricted via Customizing settings. The search help functions used should be defined in the project by consulting the person responsible for data

protection and, if necessary, the employee representation board.

4.2.11 Summary of the Key Risks

The following is an overview of the risks that tend to occur most often; they include:

- No checking or tracing options because
 - Lack of documentation on customer-specific adjustments to or configuration of the SAP System (Customizing, table maintenance, application development, and so on),
 - Maintenance of the report authorization groups has been forgotten
 - Negligent handling of the authorization concept
 - Recommendations that have not been met (such as deactivated table log, authorized programming in the production system, and so on)
- Access protection for the R/3 System is circumvented by means of programming options (in particular the authority check)
- Access protection for the R/3 System is circumvented by means of the RFC-capable function modules that are called up from an unprotected R/3 System or from external programs
- Misuse of the data via the download function and/or XXL List Viewer and subsequent processing of it for purposes prohibited by the Data Protection Act or under impermissible conditions (such as inadequate checkability)
- Infringement of the data protection requirements as a result of an unadjusted authorization concept
- Infringement of the data protection requirements as a result of additional evaluation programs, such as:
 - Using a flexible evaluation system, ABAP reports, or queries without prior agreement, that is, processing data without a legal basis
 - Changing/Extending the scope of functions for originally approved programs/ABAPs/queries
 - The programming department accessing real data in the HR department
 - Programming internal evaluations outside a R/3 application package approved by the Data Protection Act (above and beyond the facts stated in Section 4.2) which can access SAP data (for example, by means of a C program or using database tools, that is, by also circumventing the recommendations of the R/3 Security Guide)
- Changing the system status, for example:
 - Assigning access authorizations to an unauthorized user or for unauthorized programs
 - Configuring files, data fields, or keys that have not been agreed

- Creating uncontrolled interfaces between personal databases and other systems (such as controlling)
- Improperly setting the production system (for example, “changeable” status)
- Misusing data carriers, for example:
 - Evaluating data carriers with personnel data on a different SAP installation (such as a service processing center) or on other PCs
 - Misusing backup copies
- Concealing infringements by changing the system parameters, for example by:
 - Falsifying log files,, for example by temporarily deactivating table logging. This, however, requires access to the profile parameters, the table activation authorization, or the developer authorization
 - Circumventing the access authorization check by deactivating the authorization check
- Circumventing the access authorization check and logging systems by means of PC download and evaluating outside functioning security mechanisms.

4.3 Summary of the Check Procedures

In addition to the SAP topics discussed above, the following section discusses further checks that concern data protection requirements in more general terms. More information on these requirements is available in the general literature (see the bibliography in the appendix).

Implementing the necessary organizational and technical measures in order to meet data protection requirements, and the ability to check the installation are the two essential requirements for processing personal data. The organizational and technical measures required must be examined individually by each user department for each form of processing and for each processing purpose when a system is planned (see the details in Section 1 of this guide).

As varied the questions regarding the checks may seem, some issues have not been addressed here. These issues include checking the principle of data avoidance and checking the processing authorization, for example, for transferring personal data to other countries. Such issues should generally be dealt with as part of the advance checks, that is, a one-off check before the relevant system is commissioned.

In short, this means that the measures that are required or appropriate with regard to the issue of whether certain processing forms are allowed must be examined on an individual basis with regard to the following points.

In the following checklists, the different check fields from this Section are divided into three categories:

- Checking requirements, see Section 4.3.1

- If applicable, separate technical and organizational requirements resulting from priority legal specifications, for example, from company or service agreements, see Section 4.3.2
- Requirements of data protection measures pursuant to Article 9 of the German Federal Data Protection Act and the appendix, see Section 4.3.3

The issues have been described in such a way that the information is transparent for occasional system users. The description often refers to the Audit Information System and its functions. For this reason, it is recommended that the documentation on the system audit also be used to assist in preparing the checks.

4.3.1 Checking Requirements

4.3.1.1 Hardware

The documentation currently contains information on:
<input type="checkbox"/> Which SAP-relevant IT procedures (that receive data from SAP R/3 or that send data to R/3, such as time recording systems) are run on which computers?
<input type="checkbox"/> Which computers run the SAP R/3 test, quality assurance, and production systems? Does this information match the SYSTEM>>STATUS and the TSYST tables (display via SM31 or SE16)? / T000 and T001
<input type="checkbox"/> Which operating system is installed on these computers? See SYSTEM>>STATUS in the different systems.
<input type="checkbox"/> Which computer systems are used (whether Windows, UNIX, MVS, or AS/400 computers are used as the server, which client computers are in use)?
<input type="checkbox"/> Which network components (for example, routers) are used?
<input type="checkbox"/> Who is responsible for maintaining the computer operation?
Is an up-to-date network overview available in graphical and/or written form?
Is a corresponding up-to-date configuration overview and/or network description available?

4.3.1.2 Operating System and Low-Level Software

The following is documented:

- Which operating systems (and version number) are used? Compare with ".ys" in the command field or SYSTEM>>STATUS in the different systems
- Which database systems or data management systems (and release) are used? Compare with SYSTEM>>STATUS in the different systems.
- Which network operating system is run?
- Which network services are active in the server domain and which are deactivated?
- Which routers and firewall systems separate the SAP server domain and the SAP network from other networks (in particular external networks)?

Is network encryption used? If so, on which routes?

- Between application servers
- Between application servers and clients
- Between application servers and printers
- Which maintenance accesses are provided, in particular for remote maintenance (hardware or software maintenance)?

Which access rights are set up (for whom) on the R/3 database?

Is a database query language used on the R/3 database?

If so, do the purposes jeopardize the integrity and checkability of the R/3 system?

Is use of this query language unrestricted (for example, also for changing the data basis)?

Does anyone else other than system administrators have access to SAP tables and the R/3 database from operating system level?

Check the assigned access rights for SAP Objects at operating system level and at the level of the network of the servers concerned.

4.3.1.3 Programming Techniques

Do binding program guidelines exist?

Are the following stipulated

1. Which programming languages are used outside SAP and these programs can access SAP (for example, SQL, JAVA...)?
2. Which program generators or other software engineering tools are used in R/3 (ABAP Query, Report Painter, and so on)?

In which systems/clients may/can programming take place?

1. Check the client settings for changeability and recording obligation in the table T000 on each system in question
2. Check the assigned authorizations for the object S_DEVELOP activity 01 (create) and 02 (change), and PROG

In which systems/clients may/can Customizing settings be changed?

1. Check the client settings in table T000 on each system in question.
2. Check the assigned authorizations for the object S_TABU_DIS activity 02; S_TABU_CLI "X".

Is the procedure for changing the production programs stipulated in writing?

Who has which authorizations in the Change and Transporting System (CTS)? Use the Authorization Information System SUIM (users by authorization values) to analyze the assigned authorizations for the authorization object S_TRANSPRT.

Are there any Customizing tasks and programs that are not adequately documented and described?

Is the completeness of the documentation and its revision capability taken into account for all the essential changes and when upgrading the release?

Use the CTS Information System (transaction **SE03**) to analyze whether the transported customer-defined objects are adequately and clearly documented.

Is protected personal data transferred from the productive SAP System to an open information warehouse for general evaluation?

Testing Programs and Customizing Settings

Is especially created internal test data or real data used to carry out test runs?

Perform a random check on the data (for example, by calling up the relevant master and transaction data in the modules concerned) in the quality assurance client in the consolidation system.

Is it ensured that a test run using real data is only carried out in the following cases:

- Within the scope of the purposes and with the same authorizations that the testers have in the real system?
Use SUIM to analyze the authorizations in the test system.
- Within the scope of the dual verification principle, provided that above and beyond the roles of the testers (programmers, quality assurers, department), more extensive rights are assigned to the data (for example, all rights for the head of personnel)?
- With the involvement of the department that is the owner of the data?

Is it ensured that the non-anonymous test material, with the exception of the test data to be documented, is safely destructed?

Are testing tools (such as SAP internal Computer-Aided Test Tools (CATT)) used and by whom?

Use the authorization information system SUIM to analyze the user master records

Is the following stipulated?

- Which data may be used for testing programs and for performing the final test in the systems and clients upstream of the production system? Check the PLANNED specifications (of a required test concept) for conformity with the transports carried out to the consolidation or test system and their clients (transaction **SE03** or using the AIS report RSWB0040).
- Who provides suitable test data?
- Which “anonymizing” procedures are used?
- Must “anonymized” test data be used?
- Which department is responsible for formulating the programming and change requests?

Are external persons used for testing the program and for program maintenance?

Are there any special specifications for security measures to be complied with (for example, for protecting the documentation from being overwritten in the case of client copies)?

In particular, check the delivery and transport routes, as well as the assigned authorizations in the clients used for test purposes.

Program Documentation

Is the machine-assisted documentation used for developing customer objects?

Use transaction **SA38** (GOTO>>DOCUMENTATION) or **SE38** to examine the Z and Y reports and use **SE11** to examine the table documentation for the Z and Y tables.

Does the documentation describe

- Which program calls up which other programs
- Which tables are processed
- Which authorization checks are provided
- Which input values are allowed
- The other components of the object?

Is it ensured that all program changes and changes to the tables controlled by programs are recorded by granting the authorizations (object S_TRANSPRT) in a restrictive manner and by setting the systems and clients accordingly?

Does assigning the appropriate rights ensure that the documentation is protected?

Which persons have developer rights (such as S_CTS_DEVELO), who has administrator rights (such as the profile S_CTS_ALL), and who has project manager rights (for example, the profile S_CTS_PROJEC), or similar rights? Use SUIM to check the authorization object S_TRANSPRT.

Or, if necessary, can anyone release and carry out all transports on the basis of general authorizations (such as SAP_ALL)?

Are the CTS files adequately protected at operating system level?

Check the access authorizations for the SAP transport files in the directory \usr\sap\trans at operating system level

Has each program been documented with at least the following?

- Application areas of the program
- Structure and description of the program
- Process descriptions (if required)
- A data flow plan
- A description of the check tables or the view structure
- A description of the integration relations
- Screens, forms used
- A program list (most recent version)
- A log of the final test and a signed exception log
- The test data used
- Instructions for scheduling and post processing work

For this purpose, call up the online documentation (**SE38** DISPLAY documentation) and check the program files for the programs developed internally.

Is there a manual that contains all the information necessary for using the adapted R/3 System and that adequately explains the meaning of the required input data?

Check the user and training manuals.

Have the systems (table TSYST) and clients (table T000), and delivery routes (table TASYs), consolidation routes (table TWSYS), and transport layers (table DEVL) been adequately documented, and do the system settings (for example, the system changeability in T000) ensure that they are maintained?

Are the RFC interfaces adequately documented and protected?

- Which authorizations are assigned for the object S_RFC, and which users have these authorizations?
- Is the profile parameter auth/rfc_authority_check set to 1 or 2? Is the profile parameter snc/accept_insecure_r3int_rfc not set to 1? Is profile parameter snc/accept_insecure_rfc set to 0? Use report RSPARAM to check this.
- Use transaction **SM58** to analyze the RFC log for undocumented RFC calls

Are the ALE interfaces adequately documented and protected?

- Which authorizations are assigned for the objects S_ALE_* and which users have these authorizations?
- Have all ALE users been declared as CPIC users?

Are the batch input interfaces adequately documented and protected?

Which batch input users have been created for which tasks? Use SUIM to check the user master records for unknown batch input users

Release Procedures

Has an organizational procedure been developed for releasing new or changed functions in order to process protected personal data, and has the release procedure been protected with the appropriate access rights in the CTS? Have the data backup and data protection interests been adequately taken into account? Check whether organizational regulations have been implemented by appropriately assigning the authorizations for the object S_TRANSPRT.

Is the following documented?

- Who is responsible for releasing the program in line with the Data Protection Act, and, in particular, who is responsible for checking the legal basis, the necessary technical and organizational measures (special authorization checks), and the documentation?

Check this against the authorizations assigned for the object S_TRANSPRT.

- Who provides the data for the program run?

Is a release log created?

Use transaction **SE03**, report RSWBOSSR to check the texts documenting tasks.

Is the transfer of released objects to the production clients stipulated?

Check the assigned authorizations for the object S_TRANSPRT: who can carry out appropriate transports?

Are the test routines and runs sufficiently documented for checking that the procedure has been installed correctly and that the program runs correctly?

Application Development

Is the following documented?

- Which persons are responsible for ABAP/query/Ad Hoc Query development?
- Which persons are responsible for release upgrades and for maintaining the SAP procedure?
- Which parts of the procedure have been developed internally and which have been developed by a software company?

Is adequate documentation provided with regard to the following?

- Since when has each SAP procedure been used in production
- When major changes were added to the procedure (new modules, functions, and applications added)
- Who is responsible for requesting procedure changes
- How such changes must be executed in general and in emergencies

Is there a summary and a brief description of the SAP procedures deployed at different times?

User Service/System Administration

Is the following defined?

- Who is responsible for operating the computers (system administration)?
- Who is responsible for administrating the procedure?

Use transaction **SUIM** to check the information against the user authorizations.

Have the system administration actions been logged adequately?

Is it stipulated who and when this log is to/can be evaluated, and for what purposes?

Check how the logs are used and evaluated.

Have all the procedure changes been automatically adequately logged (in the CTS and by means of change logs)?

Use SE03 to check the recording obligation, in particular, in the clients concerned (table T000) as well as whether logging is complete in the CTS

Have these logs been stored in such a way that they are adequately protected against manipulation?

Check the assigned rights of access to the CTS files, who can archive and/or delete the logs at SAP and operating system level (SCD0 action 06).

Is the following documented outside the R/3 System?

- Which persons manage the authorizations (details on these persons)?
- Which data the user service has access to, or who can carry out a trace process (transaction **ST01**)?
- Which data is logged for these accesses?

Use transaction **SUIM** to check this information.

Are malfunctions and measures for eliminating these malfunctions documented in a malfunction log book outside the SAP R/3 system with provision for revisions (date, time)?

Are the steps involved in of user and authorization administration (configuring, assigning passwords, assigning rights, deleting/changing during transfer or removal) adequately documented and sufficiently organized in good time?

Computer Center Operation

Is the system console located in a protected area and protected against misuse?

Can today's date be changed?

Must all changes to the data processing system and to the system programs on which SAP Software runs be logged?

Is the system administrator's password for the systems concerned changed regularly and is it kept suitably confidential?

Is accounting

- Used in the SAP System?
- Used outside SAP?
- Is the evaluation procedure regulated?

Are there any computer center reports for checking the breaches of security ascertained?

Are these reports regularly evaluated by the revision department and/or the person responsible for data protection?

Are any operator instructions available on how to respond to system messages (user instructions)?

Are layers logged and are there any regulations governing

- Management?
- Evaluation?
- Storage?

Are there any storage and deletion periods for the computer center documentation (logs, work schedules, and so on)?

Is any documentation available for emergencies?

Have the processes been clarified for using an alternative installation?

Has the assignment of user authorizations been regulated for using an alternative installation?

Are there generally two employees present in the computer room per shift?

Are functions controlled in sensitive areas?

4.3.1.4 Applying the Procedure

Check also the data backup measures in accordance with Article 9 of the German Federal Data Protection Act in paragraph 3 of the checklists.

4.3.2 **Checking Special Regulations from Priority Legal Specifications (for Example, from Valid Company Agreements on Organizational and Technical Measures)**

Appendix on User Authorizations

Is the appendix kept up to date?

Is the appendix managed manually or using the system?

If the appendix is generated automatically, perform the check with the corresponding function:

- Use report RSUSR002 to gain an overview of the users and the assigned profiles
- Use report RSUSR002 to evaluate a specific object if you only want to search for users with access to certain authorization objects
- Use report RSUSR003 to check the standard users
- Use reports RSUSR008 and RSUSR009 to check the users who have critical authorizations.

Depending on the form of the appendix, compare the list with the current status of the tables (by means of **SA38** and the corresponding RSUSR* ABAPs).

If necessary, compare the TARGET and ACTUAL status of the appendixes in the form of PC files in the .dbf or .xls format with a corresponding MS Query SQL Query.

Compare also the further access protection checks under the column 'Checking Data Protection and Data Backup Measures in Accordance with Article 9 of the German Federal Data Protection Act'.

4.3.3 Checking the Data Protection Measures in Accordance with Article 9 of the German Federal Data Protection Act and the Appendix

When the technical and organizational measures implemented in accordance with Article 9 of the German Federal Data Protection Act and the appendix to this Act are checked, the appendix numbering system is used, even if this sometimes leads to individual check points being listed twice. Only those points relating to SAP Software are listed. The key points are “Access control”, “Order control”, and “Availability control”. These points deal with areas that must be solved by other technical or organizational means outside the SAP System. Where appropriate, some checks are also included here for such cases.

4.3.3.1 Item 1: Access Control

According to Item 1, ‘Unauthorized persons must be denied access to data processing systems that process or use personal data (**Access control**)’.

This requirement is not relevant to SAP R/3.

4.3.3.2 Item 2: Access Control

Item 2 of the appendix to Article 9 of the German Federal Data Protection Act stipulates that ‘the use of data processing systems by unauthorized persons must be prevented (**Access control**)’

Authentication

Is it ensured that all SAP users have their own user master record?

Perform random checks to establish whether all users in the departments concerned are in the list of authorized users (report RSUSR002).

Use RSUSR002 to perform further checks on the list of users for possible general users, for example, 'warehouse' or 'personnel administrator', or similar.

- Are there any specifications for secure passwords? Are the illegal passwords adequately maintained in table USR40?
- Are there any minimum requirements for the length and structure of passwords (recommendation: min. 6 characters)? Which settings are available for the minimum password length? Use RSPARAM to check the parameter login/min_password_lng.
- Are users automatically forced to change their password? Which settings are defined for changing the password? (recommendation: 60 or 90 days). Use RSPARAM to check the parameter login/password_expiration_time.
- Is the connection terminated after a certain number of failed attempts (3)? Use RSPARAM to check the parameters login/fail_to_session_end and login/fail_to_user_lock.
- Is the automatic creation of the SAP* user deactivated? Use RSPARAM to check the parameter login/no_automatic_user_sapstar (the value should be 1 when the user is deactivated).
- Are inactive users automatically logged off? Use RSPARAM to check the parameter rdisp/gui_auto_logout.
- Have the standard users SAP*, DDIC, SAPCPIC, and EARLYWATCH been adequately protected? Use RSUSR002 to call up their user master records and analyze the results of RSUSR003.
- Use report RSUSR200 to check inactive users with initial passwords.

Are other methods used, for example, chip cards, for authentication on the frontend computer when the computer is in more or less publicly accessible rooms?

Can the user use the software to block his screen without logging off? Is the password protection activated at PC operating system level, in particular at locations open to the public?

Is the screensaver activated when the screen is inactive for a long period of time? After how many minutes? In particular, check the computers that are accessible to the public.

Is special security software used to ensure data security on the PCs?

Is the SAP data encrypted by means of Secure Store & Forward (SSF), and which data is encrypted?

Is it ensured that protected data cannot flow to unprotected systems from the SAP R/3 System via the download function and/or mail?

Check the authorizations assigned for the object S_GUI.

Use XXL List Viewer functions to check access to programs.

Is it ensured that access for remote maintenance (in client 066) can only be granted when remote maintenance is explicitly requested?
Are the configured user master records locked for the rest of the time?
Is logging activated (transaction **SM19**) during remote maintenance?
Is the log subsequently evaluated?

4.3.3.3 Item 3: Access Control

Thirdly, it must be ensured that persons authorized to use a data processing system can only access the data they are authorized to access and that personal data cannot be read, copied, modified, or removed without authorization during processing or use, or after it has been saved (**Access control**).

Access Protection

Are users/functions/rights assigned?

In addition to the overview of users in RSUSR002, is there also a table that identifies the current status of users and authorizations?

Is the user group differentiated in the authorization master record, that is, is it maintained by department or in relation to cost centers? Use RSUSR002 >Display all users> 'other view' to analyze the user groups.

Are the comprehensive general authorizations (such as SAP_ALL) restricted to protect emergency users (with compulsory logging)?

Use the Authorization Information System (transaction **SUIM**) to check who has the composite SAP_ALL profile and who has comparable comprehensive authorizations.

Check whether compulsory logging is activated for these users in the production environment (transaction **SM19**).

If necessary, check the logs in the production environment for suspicious use of comprehensive authorizations.

Are the sensitive tables adequately protected by table authorizations? Analyze the table classes in the table TDDAT for the authorization object S_TABU_DIS.

Use **SUIM** >> users by authorization values for S_TABU_DIS to subsequently check which users have access to these table classes.

Are the sensible programs adequately protected by report classes? Use report RSCSAUTH to analyze the report classes assigned for the reports to be protected.

Alternatively, are only report trees accessible to the end user? Check whether the use of the transaction **SA38** is protected.

Are all the transactions that are to be protected either locked (view using report RSAUDITC) or provided with an authorization check for the object S_TCODE? Analyze table TSTCA or use transaction **SE93**.

Is the scope of the authorization check reduced in critical transactions, if required? Check the parameter `auth/no_check_in_some_cases`. If the parameter value is Y, use SU24 to determine which checks have been deactivated/changed.

Is it ensured that the dual verification principle is applied for maintaining and activating authorizations and profiles, and for maintaining users?

Check the organization and settings for the objects `S_USER_GRP` (in particular: who can maintain which user groups?), `S_USER_PRO`, and `S_USER_AUT`.

Is the operating system level locked for the users?

Use report `RSPARAM` to check the parameter `rdisp/call_system`. If the value is not set to 0, the operating system can be accessed from SAP.

Is there an organizational division between application development, work scheduling and post processing, data input, operating, and archive management? In particular, analyze the assigned authorizations for the object `S_TRANSPRT`.

Was the program switch for using the structural authorization configured each time in accordance with the regulations?

Check the use of the program switch for structural authorizations in the HR module in table `T77S0`.

Was the authorization concept adequately tested before startup?

User Interface

Are the users specifically directed to the relevant sub-menu by means of a corresponding entry in the user master record? Call up report `RSUSR002`, generate a list of all the users in question, click the 'other view' button, and check the 'start menu' column.

Does Customizing ensure that users only have access to the data they need to carry out their tasks?

Use `PA20` in Human Resources, for example, to check the masks (screens) that the individual users can access.

Check the Customizing settings for the topic: "Customizing Interface".

Logging

Is the usage data logged by the operating system in such a way that it can be determined who outside SAP has accessed which SAP R/3 data, when, how, and with which resources?

Is the download logging function activated in the security log?

Is download logging regularly evaluated in `SM20` in accordance with the Data Protection Act?

4.3.3.4 Item 4: Transfer Control

Fourthly, it must be ensured that during electronic transfer, transporting, or storage on data carriers, personal data cannot be read, copied, modified, or removed without authorization and that it can be checked and established where a transmission of personal data is provided for by means of data transfer equipment (transfer control).

Access Protection

Are users/functions/rights assigned?

In addition to the overview of users in RSUSR002, is there also a table that identifies the current status of users and authorizations?

Is the user group differentiated in the authorization master record, that is, is it maintained by department or in relation to cost centers? Use RSUSR002 >Display all users> 'other view' to analyze the user groups.

Data Transfer

Is an overview/list kept of the departments where data transfer can be controlled by programs?

Call up the Audit Information System (transaction **SECR**) and check SYSTEM AUDIT>>SYSTEM CONFIGURATION>>SYSTEM, and >>R/3 COMMUNICATION TYPES for the RFC, CPIC, and ALE connections.

If necessary, also check external access authorizations.

Is there up-to-date documentation on the programs to be used for automatic transfer in accordance with Article 10, paragraph 4 of the German Federal Data Protection Act outside SAP R/3?

Are the program-controlled transfers logged outside SAP R/3 in a revision-secure manner by means of recording

- The transferring users
- The recipients
- The data
- The date
- The time?

Does SNC encrypt the data on the transfer routes?

If so, between which instances (SAP GUI and the application server, the application server and the printer, and so on)?

Output Management

Is the information that can be output to PCs documented? Check the assigned authorizations for the object S_GUI (activity 61).

Are the printouts user specific during the processing of personnel data? Are the printer authorizations configured with regard to the department or the user, or can copies be made inadvertently in external departments/locations/countries?

Check the authorizations for the object S_SPO_DEV and their assignment.

4.3.3.5 Item 5: Input Control

Fifthly, it must be ensured that subsequent checks can be made to establish **whether and by whom** personal data was entered, **modified, or removed** in data processing systems (**input control**).

Log Settings

Which users are logged automatically?

Use report RSPARAM to check the settings for **SM19** if the rsau/enable parameter is set to 1.

Is the function for logging table changes activated? Use RSPARAM and RECCLIENT to check the rec/client and TP parameters.

Do all the key table changes have to be logged (in particular, system and key tables, such as the table of reasons for absence T554*)?

List all the tables in question and check the settings (transaction **SCU3** or display the table DD09L)

Are the program-controlled transfers logged outside SAP R/3 in a revision-secure manner by means of recording

- The user entered (name)
- The date and time of creation
- The data created

Use transaction **SCD0** to check the change documents set for all the objects in question.

Is nobody authorized to delete the change documents?

Use the Authorization Information System SUIM or the report RSUSR002 to check which users have activity 06 for the object S_SCD0.

Log Analyses

Which logging function is used in the SAP R/3 procedure by whom and for what purposes?

- Is the Security Audit Log activated and why? Use report RSPARAM to check transaction **SM19** and the rsau/enable parameter (value must be 1).
- Check the system log for incorrect logons (transaction **SM21**).
- Are the daily statistics (transaction **STAT**) used if necessary? See the parameter stat/level = 1.
- Which application logs are activated? Compare the configuration SLG0 for the SLG1.
- Who can use the function for logging workflows (transactions **SWI2** and **SWI5**), and for what purpose?
- For which business objects is logging activated? (transaction **SCD0**)
- Logging tables (transaction **SCU3**)
- Check the change logs for users, profiles, and authorizations (transaction **SUIM**)

4.3.3.6 Item 6: Order Control

Item 6 stipulates that it must be ensured that personal data to be processed in the order can only be processed in accordance with the instructions from the sold-to party (**order control**).

Access Protection

Are users/functions/rights assigned for the contractor?

In addition to the overview of users in RSUSR002, is there also a table that identifies the current status of users and authorizations at the contractor?

Is the user's user group differentiated in the authorization master record for the contractor, that is, is it maintained by department or in relation to cost centers? Use RSUSR002 >Display all users> 'other view' to analyze the user groups.

Are the contractor's authorizations restricted to a minimum?

Is it ensured that adequate checks cover the risks of comprehensive authorizations for the contractor?

4.3.3.7 Item 7: Availability Control

Item 7 stipulates that it must be ensured that personal data is protected against accidental destruction or loss (availability control).

Access Protection

Are sufficient, regular backup runs provided?

Is it ensured at operating system level that SAP files cannot be inadvertently deleted? Are the access rights restrictively assigned at operating system level in accordance with SAP recommendations? Are the available access rights checked regularly?

Is it ensured at database system level that SAP files cannot be inadvertently deleted? Are the access rights restrictively assigned at database level in accordance with SAP recommendations? Are the available access rights checked regularly?

Is access to the archived data and data carriers adequately protected? Check the relevant organization.

Is it ensured that the data processing systems and the data carriers are adequately protected against the effects of fire, water, power failure, and power fluctuations?

Is it ensured that the data carriers are adequately protected against the effects of material fatigue? Check whether adequate random samples are taken.

4.3.3.8 Item 8: Ensuring Earmarking

Item 8 stipulates that it must be ensured that the data ascertained can be processed for various purposes.

Access Protection

Are users/functions/rights for authorized purposes assigned strictly enough at the access protection level?

For individual user groups, check the accessibility of

- The program library
- Additional functions, such as ABAP Query and Ad Hoc Query
- The download function and the XXL List Viewer
- The programming tools
- The administration functions
- The ABAP List Viewer in evaluation programs for personal data
- In particular, the logs and change documents

Other Measures

Are the users/functions/rights adequately separated at the level of the individual systems, clients, and company codes?

Are the remaining risks covered by appropriately training the users in the departments, in programming, and in system management?

4.3.3.9 Other Checks

The introductory paragraph to the appendix to Article 9 of the German Federal Data Protection Act also demands for ‘the intra-authority or intra-organization to be implemented in such a way that it meets the specific requirements laid down in the Data Protection Act’. This requirement should be monitored by performing the following checks:

General Guidelines

Are there any guidelines governing data security (in general or especially for the IT procedure), and are these guidelines up to date?

Are all the persons involved appropriately informed of these guidelines?

Are any evaluations carried out following breaches of security?

Which logs have been created by whom?

Does the procedure ensure that any lack of technical and organizational measures or breaches of data protection are immediately forwarded to the person responsible for data protection in the company and that corrective action can be taken in conjunction with this person?

Has a risk and weak point analysis been carried out?

Access Management and Log Analyses

Are the access authorizations of a user who is leaving the company or who is to be transferred elsewhere deleted immediately? Is there an automatic workflow for deleting users (if necessary)?

Are the user master records, authorizations, profiles, and, if applicable, roles adequately automatically managed and maintained, and immediately regulated?

Check the authorization framework concept and the organizational management in user administration, and maintain profiles, authorizations, and roles.

Is the revision capability of the access authorizations taken into consideration?

Does the internal control system regularly check the observance of the authorization concept? How often are such checks performed?

Are there any sanctions governing identified misuses and attempts to misuse systems?

Is the logging of all unsuccessful attempts to log on as a user (report RSUSR006) checked regularly?

Is the transfer of printouts to users regulated, if these users do not have a work center printer?

Are the authorizations to access printers sufficiently restricted?

Is the backup method at database level documented in writing?

Have the backup files been protected by a password or a release date, for example?

Are the configured protective measures regularly subject to a thorough test to establish whether they still fulfill the desired protection purpose?

Index

- ABAP 12, 31
- ABAP List Viewer 27, 28
- Access authorizations. 19, 31, 36, 45, 48, 49
- Access control 7, 41, 43
- Access protection .. 20, 40, 43, 45, 46, 47
- Accounting 39
- Activation administrators 22
- Administration 19, 22, 24
- Advance checks 32
- ALE 26, 27, 28, 37, 45
- Audit Information System 28, 33
- Audits 20, 28, 29, 45
- Authentication 9, 20, 41
- Authority groups 16
- Authorization checks . 10, 11, 14, 15, 17, 20, 21, 28, 36, 38
- Authorization concept 6, 7, 8, 15, 17, 19, 21, 22, 27, 30, 31, 44
- Authorization framework concept 49
- Authorization groups 14, 21
- Authorization objects . 13, 17, 18, 20, 21, 22, 23, 27, 28, 40
- Authorizations 6, 7, 8, 12, 14, 16, 17, 18, 19, 20, 21, 22, 23, 24, 27, 28, 30, 34, 35, 36, 37, 38, 40, 42, 43, 44, 45, 47, 49
- Availability control 6, 8, 41, 47
- BAPI 26, 27
- Batch input 26, 27, 37
- CATT 35
- CCMS 12, 29, 30
- Central user maintenance 22
- Checklists 28, 32, 40
- Checks 17, 18, 20, 26, 27, 30, 47
- Computer center operation 39
- CTO 15, 24
- CTS 15, 24, 35, 36, 38, 39
- Customizing ... 19, 20, 22, 24, 25, 31, 35, 44
- Data categories 27
- Data fields 19, 31
- Data security 42, 48
- DDIC 12, 42
- Deletion 47
- Deletion periods 27
- Development system 24, 25
- Documentation . 8, 13, 24, 29, 31, 33, 35, 36, 37, 38, 45
- Downloading 32, 42
- Downloads 7, 11, 17, 27, 28, 31
- EarlyWatch 13
- Earmarking 6, 7, 27, 47
- Emergency users 20, 29
- Employee representation board 16, 31
- Encryption 7, 42, 45
- German Federal Data Protection Act
 - § 4e German Federal Data Protection Act 27
 - § 4g German Federal Data Protection Act 27
 - § 9 German Federal Data Protection Act 6, 7, 33, 40, 41, 48
 - §10 German Federal Data Protection Act 45
- HGB 16
- Identification 9, 20
- Infotypes 13, 14, 16, 17, 18
- Initial password 11, 12, 13, 42
- Input control 8, 45
- Locking 12, 13, 29
- Log files 32
- Logging 16, 28, 32
- Logs 24, 25, 26, 28, 29, 30, 39, 40, 43, 48
- Maintenance 38
- Misuse 6, 27, 32
- Monitoring 11, 13, 21, 27
- Order control 8, 41, 46
- Password protection 7, 42
- Passwords 9, 10, 11, 12, 30, 42, 49
- Preliminary check 6
- Production system 6, 9, 18, 19, 23, 24, 25, 26, 31, 33
- Profile generator 10, 13, 23
- Profile parameters 9, 10, 11, 29
- Profiles 12, 13, 18, 19, 22, 23, 40, 49
- Prohibited purposes 31
- Quality assurance system 24

Queries	31	TSTCA	15, 43
Recipients.....	45	TSYST	33, 37
Report		TWSYS	37
MPPAUTSW	20	USR40.....	9, 11, 42
RHAUTUPD_NEW.....	23	V_T599R.....	30
RPLIC010	30	Technical and organizational measures 6,	
RPLMIT00.....	30	38, 48	
RSCSAUTH.....	15, 21, 43	TMS	24, 25, 26
RSPARAM	11, 28, 37, 42, 44, 46	Transaction	
RSSTAT020.....	29	PA30	14
RSSTAT026.....	29	PFCG.....	13
RSUSR002..	40, 42, 43, 44, 45, 46, 47	PFUD	23
RSUSR003.....	40, 42	RZ10	9, 11
RSUSR006.....	49	RZ11	9, 11
RSUSR008.....	40	SA38	15, 21, 36, 40, 43
RSUSR009	40	SCD0.....	16, 39, 46
RSWB0040	36	SCU3.....	46
Repository	25	SE03.....	24, 35, 36, 38, 39
Revision	28, 39	SE06.....	25, 26
RFC	11, 26, 27, 31, 37, 45	SE11	36
Risks9, 10, 11, 13, 17, 19, 21, 23, 26, 27,		SE13.....	25
30, 31, 47, 48		SE16.....	11, 15, 16, 21, 33
Risks.....	26	SE38.....	15, 36, 37
Role administrators	22	SE80.....	15
Roles	12, 13, 22, 23, 29, 49	SE84.....	15
SAP Facts.....	9	SE93	43
SAP Logon.....	9	SECR.....	28, 29, 45
SAP Note		SM19.....	20, 29, 43, 46
28777.....	17	SM20.....	20, 29, 44
29276.....	12	SM21	29, 46
SAP Service System	21	SM30.....	16, 25
SAPCPIC	12, 42	SM58.....	37
Search help.....	14, 30	SM59.....	27
Security Audit Log.....	20, 29, 30, 46	ST01	39
Security Guide	8, 11, 12, 31	STAD	29
SNC.....	11, 45	STAT.....	29, 30, 46
Storage periods.....	24, 26	STMS	24
Syslog.....	29	SU03	13
Table		SU24	10, 44
DEVL.....	37	SUIM.....	13, 35, 36, 37, 38, 39, 43, 46
T000	25, 26, 33, 34, 35, 37, 39	SWI2	30, 46
T001	33	SWI5	30, 46
T599R	30	SWU9.....	30
T77S0.....	20, 21, 44	Transactions ...	10, 11, 13, 14, 15, 16, 21,
TASYS.....	37	23, 25, 26, 28, 29, 35, 36, 38, 39, 43,	
TDDAT	43	45	

Transfer 7, 32, 44, 45
Transfer control..... 7, 44

User administrators 22, 23
XXL List Viewer 7, 17, 31, 42, 48