SAP AG
Neurottstr. 16
D-69190 Walldorf

R/3 Security

R/3 Security Guide : VOLUME III

Checklists

Version 2.0a : English

November 24, 1998

Copyright

SAP AG further does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP AG shall not be liable for any special, indirect, incidental, or consequential damages, including without limitation, lost revenues or lost profits, which may result from the use of these materials. The information in this documentation is subject to change without notice and does not represent a commitment on the part of SAP AG in the future.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

SAP AG assumes no responsibility for errors or omissions in these materials.

Copyright

Table of Contents

Chapter 1 : Introduction

Chapter 1-1 : How to Use the *R/3 Security Guide*

The *R/3 Security Guide* consists of three separate volumes, with different levels of detail:

R/3 Security Guide VOLUME I : An Overview of R/3 Security Services

R/3 Security Guide VOLUME II : R/3 Security Services in Detail

R/3 Security Guide VOLUME III : Checklists

R/3 Security Guide VOLUME I : An Overview of R/3 Security Services

The *R/3 Security Guide VOLUME I* provides a general overview of the security services that we offer in R/3. With *VOLUME I*, you can familiarize yourself with these services, for example, before establishing a security policy or before installing an R/3 System.

<u>R/3 Security Guide VOLUME II : R/3 Security Services in Detail</u>

This part of the *R/3 Security Guide* concentrates on the technical measures involved with R/3 System security. It contains descriptions of the tasks involved, as well as our recommendations for the various components of the R/3 System. Use *VOLUME II* once you have established a security policy and are ready to implement it for your R/3 System.

<u>R/3 Security Guide VOLUME III : Checklists</u>

The third part of the *R/3 Security Guide* complements *VOLUME II* with checklists. You can use these checklists to record those measures that you have taken and for assistance when reviewing and monitoring them.

<u>Updates</u>

We will also publish updates to the guide as necessary. These updates will also be available over SAPNet in regular intervals.

The R/3 Security Guide VOLUME III : Checklists

You are currently working with the *R/3 Security Guide VOLUME III : Checklists*. The prerequisites for using this volume are:

- An existing security policy
- A good understanding of the concepts and measures to take as described in the *R/3 Security Guide: VOLUMES I* and *II*.
- Time and resources

  Security is not only an aspect of quality; it is also an aspect of protection. Insufficient security can result in loss of time, assets, money - or your business! Security is an investment - of both time and resources. We recommend you dedicate sufficient time and allocate ample resources to implement your security policy and maintain the level of security that you desire.

Using VOLUME III

The checklists provided in this volume are a summary of the measures that we previously described in the *R/3 Security Guide: VOLUME II*. We provide these checklists as samples of the various security items that you can consider for your security policy.

☞ **Note**

Keep in mind the following points of advice:

- Regard these checklists as suggestions and examples! These checklists **do not in any way** represent a complete collection of items that apply to everyone.
- Copy these checklists and modify them to comply to your individual security policy.
  - Define your own priorities.
  - Delete those items that do not apply to your needs.
  - Add any items that you find necessary that we have not included.
- Update your checklists regularly to adjust them to changing needs.

Our **Security Consulting Team** is also available for assistance. See *Chapter 1-2 : Support and Feedback.*

Valid Releases

This version of the *R/3 Security Guide* applies to R/3 Releases 3.0, 3.1, and 4.0. Where applicable, references to other releases are explicitly indicated.

Typographical Information and Standard Notations

The following tables explain the meanings of the various formats, symbols, and standard notations used in the guide.

Table 1-1 : Typographical Information Used in this Guide

This text format	helps you identify
Screen Text	words or characters you see on the screen (this includes system messages, field names, screen titles, menu names, and menu items).
`User Entry`	exact user input. These are words and characters you type on the keyboard exactly as they are in the documentation.
`<Variable User Entry>`	variable user input. Pointed brackets indicate that you replace these variables with appropriate keyboard entries.
ALL CAPITALS	report names, program names, transaction codes, table names, ABAP language elements, file names, and directories.
Book Title	cross-references to other books or references.
KEY name	keys on your keyboard. Most often, function keys (for example, F2 and the ENTER key) are represented this way.
`Technical Object Name`	names of technical objects outside of the R/3 System (for example, UNIX or Windows NT filenames or environment variables).

This icon	helps you identify
Example	an Example. Examples help clarify complicated concepts or activities.
Note	a Note. Notes can contain important information like special considerations or exceptions.
Caution	a Caution. Cautions help you avoid errors such as those that could lead to data loss.

Table 1-2 : Standard Notations used in this Guide

This Notation	helps you identify
<sid>, <SID>	the three character System ID; lower and upper case respectively.
<SYS>	the R/3 System number
<sid>adm, <SID>ADM	the R/3 System administrator at the operating system level; lower and upper case respectively. Exception: Under AS/400, the system administrator is the user <SID>OFR.

Chapter 1-2 : Support and Feedback

Technical Consulting Services

If the *R/3 Security Guide* does not satisfactorily answer all of your questions, or if additional questions arise, our Security Consulting Team within the SAP Technical Consulting Services is available for assistance.

We currently offer the following services:

- Support and consulting services when establishing a company-wide security policy
- Security analysis services
- Individual consulting services on security in the R/3 environment
- Support services when establishing a Windows NT domain concept
- Consulting services when using the Internet Transaction Server
- CA900 Course: Technical Revision - System Security
- Workshop on the R/3 Authorization Concept

For further information, contact the Security Consulting Team at:

Tel: **+49 6227 / 7-41537**
Fax: **+49 6227 / 7-44640**

For more information, see:

- Fact Sheet: *Technical System Security*, Material Number: 50026500, or
- OSS Note 114045: Consulting: technical system security

Feedback

We are also interested in knowing how well the *R/3 Security Guide* meets your needs. We encourage you to provide us with your comments on the contents and quality of this guide. To do so, use the Feedback Reply Form provided at the end of the guide and return it to us at the following address or fax number:

SAP AG
CCMS & Security Department
Postfach 1461
D-69190 Walldorf
Germany

Fax: **+49-6227 / 7-41198**

Chapter 2 : Checklists

We have designed these checklists to complement those security items discussed in *The R/3 Security Guide: VOLUMES I* and *II*. However, we do not imply that they are a complete list that applies to your own security policy. We recommend that you modify these checklists to meet your own policy requirements. Add or delete items as necessary, and define your own priorities.

Note

The following guidelines apply when using these checklists:

- The numbering of the checklists correspond to the chapters in *The R/3 Security Guide: VOLUME II*.
- The **Prio.** column: Define and use your own priorities.
- In the **Method** column, we provide you with the transaction, report, or similar instructions that apply to the security item. An entry of UP x-x-x refers to the corresponding Useful Procedure in *VOLUME II*.
- The following guidelines apply to using the **References** column*:*
    - In the heading, we have included the corresponding chapter in the *R/3 Security Guide: VOLUME II*. This reference **always** applies to the items included in the checklist. Keep in mind that each chapter in *VOLUME II* also contains sources of additional information.
    - Table references also refer to the corresponding table in VOLUME II.
    - Where applicable, we have also included sources in the checklist that directly apply to the security items (for example, OSS Notes, a different chapter in VOLUME II, or the R/3 Online Documentation).
- As appropriate, we have included comments in the **Result / Comments** column. You can use this column for your own comments as well.

Checklist 2-1 : User Authentication

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-1)	Result / Comments
Passwords					
		Have you established a password policy (how complex passwords should be, how often they should be changed, etc.)? Have you informed your employees of the policy? If possible, can you technically enforce the policy?	Company policy		
		What is your minimum length for passwords?	Set the profile parameter `login/min_password_lng`.	Table 2-1-1	Default = 3
		Do users have to change their passwords on a regular basis?	Set the profile parameter `login/password_expiration_time`.	Table 2-1-1	Default = 0 (users do not have to change passwords)
		Do the system administrators and holders of other important positions use more complex passwords?			Complex passwords should be the maximum length and contain at least one digit and one special character.
		Do you prohibit certain character combinations (such as company name)?	Enter the character combinations that you want to prohibit in Table USR40 (UP 2-1-1).		
		Do you use an external security product with R/3 for authentication that takes place outside of the R/3 System?		Chapter 2-3 *SNC User's Guide* external security product documentation	By using an external security product, you can enforce longer passwords and you can eliminate the need to transfer passwords over the network.

Checklist 2-1 : User Authentication (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-1)	Result / Comments
Protecting Standard Users					
		What R/3 clients do you have in your system? Do you regularly monitor them to make sure that no unknown clients exist?	Display Table T000 with Transaction SM31 to obtain a list of all R/3 clients.		
		Have you changed the default passwords for the standard users SAP*, DDIC, SAPCPIC, and EARLYWATCH?	UP 2-1-3		You may want to lock SAPCPIC instead of changing its password. See below: *Protecting SAPCPIC*.
		Do you monitor the status of your standard users regularly?	Use the report RSUSR003 to ensure that SAP* has been created in all clients and that the passwords for the standard users have been changed.	OSS Note 40689	
Protecting SAP*					
		Does SAP* exist in all clients?	Report RSUSR003		Do not delete the user SAP*!
		Have you deactivated it in all clients?	UP 2-1-2	For information on the profile parameter, see OSS Note 68048.	Alternative: set the profile parameter `login/no_automatic_user_sap*` or `login/no_automatic_user_sapstar`- depending on release.
		Does SAP* belong to the group SUPER?			
		Is SAP* locked?			

Checklist 2-1 : User Authentication (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-1)	Result / Comments
Protecting DDIC					
		In which clients does DDIC exist?		OSS Note 11677 OSS Note 34964	DDIC is created in clients 000 and 001 during the installation process and is needed for tasks in the installation process, software logistics, and certain ABAP Dictionary tasks. It is also needed in other clients for imports. Therefore, do not delete DDIC or its profiles. Change its initial password!
Protecting SAPCPIC					
		Have you either changed SAPCPIC's password or have you locked the user? If you changed the password, have you adjusted the affected programs accordingly? If you have locked SAPCPIC, are you aware of the loss of functions?	UP 2-1-3	OSS Note 29276 Table 2-1-3	When locking SAPCPIC, the loss of functions depends on release - see the OSS Note 29276.
Protecting EARLYWATCH					
		Does the user EARLYWATCH exist only in client 066? Is EARLYWATCH locked except for when it is needed?			
Protecting the user for R/3 Online Services					
		If you use R/3 Online Services: • Do you have a procedure to activate the user for R/3 Online Services only when needed?		Chapter 2-10 in the section titled *R/3 Online Services* OSS Note 46902	

Checklist 2-1 : User Authentication (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-1)	Result / Comments
Preventing Unauthorized Logons					
		Do you monitor unsuccessful logon attempts on a regular basis (daily)?	Report RSUSR006		Report RSUSR006 shows all unsuccessful logon attempts by a known user and all user locks.
		Do you use the Security Audit Log for recording and analyzing logon attempts?	Transactions SM18, SM19, SM20	Chapter 2-9	The Security Audit Log is available as of Release 4.0.
		Have you set session termination after a number of unsuccessful logon attempts?	Set the profile parameter `login/fails_to_session_end`.	Table 2-1-4	Default = 3
		Have you activated automatic logoff for idle users?	Set the profile parameter `rdisp/gui_auto_logout`.	Table 2-1-4	Default = 0 (off)
		Do you have users locked after a number of unsuccessful logon attempts? Is the default (12) appropriate or have you changed the value?	Set the profile parameter `login/fails_to_user_lock`.	Table 2-1-4	Default = 12
		Does your R/3 System automatically remove user locks at midnight on the same day?	Set the profile parameter `login/failed_user_auto_unlock`.	Table 2-1-4	Default = 1 (yes)
		Do you regularly check the system log for locked users?			
		Do your end users use screen savers with passwords?			
		Do you use the SAP Logon Pad instead of SAP Logon?			SAP Logon Pad prevents changes to the SAP Logon configuration.
		Are there other logon checks that you want to perform?	Define your own logon checks in the customer exit SUSR0001	OSS Note 37724	

Checklist 2-1 : User Authentication (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-1)	Result / Comments
Security Measures When Using the Session Manager					
		Do you use the Session Manager under Windows NT or Windows 95 with any of the R/3 Releases 3.0E - 3.1G? If yes, have you exchanged the `slg_dll.dll`?		OSS Note 80723	
Security Measures When Using SAP Shortcuts					
		Are your front ends protected from unauthorized access?	Depends on your infrastructure and operating system.		

Checklist 2-2 : R/3 Authorization Concept

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-2)	Result / Comments
Maintaining Authorizations and Profiles with the Profile Generator					
		Have you defined job roles for your company's job matrix? Have you specified the transactions and menu paths that each job role needs to use?	Company policy	*Authorizations Made Easy Guide, IMG,* or *ASAP*	Our Security Consulting Team offers a workshop on the R/3 Authorization Concept.
		Do you have defined procedures for creating and maintaining the activity lists, profiles, and user master records?	Transaction PFCG	*Authorizations Made Easy Guide, IMG,* or *ASAP*	
Manually Maintaining Authorizations and Profiles					
		As with the profile generator, have you defined job roles for your company's job matrix?	Company policy		
		Have you determined the activities that each job role is allowed to perform, along with the proper authorizations?	Company policy		
		Do you have a standard policy for creating and assigning profiles and authorizations?	Company policy		
The Authorization Infosystem					
		Do you use the Authorization Infosystem to review your authorization plan? Do you review it on a regular basis?	Authorization Infosystem (Transaction SUIM)		
		Which authorizations do you consider critical? Which profiles contain these authorizations? Which users have these profiles or authorizations?	Authorization Infosystem (Transaction SUIM)		Examples: To find out which profiles contain certain authorizations, see *Profiles* → *List profiles by Complex Selection Criteria* → *By authorizations contained*. To users have a certain profile in their user master records, see *Cross Reference* → *Where-used lists* → *For profiles*.

Checklist 2-2 : R/3 Authorization Concept (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-2)	Result / Comments
The Authorization Infosystem (continued)					
		What other information do you consider important? Which lists do you generate to provide you with this information?	Transaction SUIM		For example, you can create lists for: • Profile comparisons • Transactions that a specific user can execute • Changes in the authorization profile for a user
Organizing Maintenance Tasks					
		Have you separated your user administration tasks into different groups so that the tasks are covered and checked by several administrators?			If you operate in a centralized environment, it may be more appropriate to have a single superuser who performs all user and authorization maintenance tasks. In a decentralized administration environment, we recommend dividing the tasks so that they are covered by several administrators.
		Do your administrators belong to the group SUPER?			Only an administrator with the profile S_A.SYSTEM can change users belonging to the group SUPER.
		Which tasks are the administrators allowed to perform and which are not? Which authorizations or profiles does each administrator have, or to which activity group does each belong?		Tables 2-2-1 and 2-2-2	

Checklist 2-2 : R/3 Authorization Concept (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-2)	Result / Comments
Authority Checks					
		Do you include authority checks in your own developments?	Transaction SE93 AUTHORITY-CHECK at program level.	OSS Note 67766 (for information on S_TCODE)	The authority check against the object S_TCODE is automatically performed in R/3 for transaction starts over the menu or command line (as of Release 3.0E).
		Do you assign reports to report classes?	Report RSCSAUTH	OSS Note 7642 Report RSCSAUTH documentation	
		Do you assign authorization groups to tables?	Assign an authorization group to tables in the Table TDDAT.		We do deliver a number of tables with pre-defined authorization groups.
Reducing the Scope of Authority Checks in R/3					
		Is it necessary to reduce the scope of authority checks? Have you carefully considered the security aspects involved?	Company policy		We advise you to consider this option carefully before suppressing authority checks.
		How is the profile parameter `auth/no_check_in_some_cases` set? Is the value set to that what you want it to be? Do you check the value regularly to ensure that it has not unknowingly been changed?			

Checklist 2-2 : R/3 Authorization Concept (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-2)	Result / Comments
Reducing the Scope of Authority Checks in R/3 (continued)					
		Do you reduce the scope of authority checks? Have you carefully determined which authority checks you want to deactivate before deactivating any?	To reduce the scope of authority checks: 1. Set the profile parameter `auth/no_check_in_some_cases` to the value `'Y'.` 2. Use Transaction SU25 to copy SAP defaults. 3. Use Transaction SU24 to change the individual values.		Only use this option for individual transactions. Do not use it for bulk changes!
		If you do reduce the scope of authority checks, then do you regularly check the deactivated authority checks to make sure that they have not unknowingly been changed?	Transaction SU24		

Checklist 2-3 : Network Infrastructure

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-3)	Result / Comments
Network Topology					
		Have you designed your network topology with security in mind?	Company policy		
		How is your network topology designed? What do you have for subnets and LANs? What servers are located in each subnet or LAN? Are your frontend LANs separated from your server LANs? What are the security requirements on each of your subnets or LANs?	Company policy		Defining your network topology is a very individual process. Our Security Consulting Team is available for assistance.
Network Services					
General Network Services					
		The following questions apply to general network services for both Windows NT and UNIX (for example, under UNIX, the services `sendmail`, NFS): • What ports are open on your servers? Which services are allowed on these ports? • Have you deactivated those network services that you do not need?	List 'open' ports with the command `netstat -a`. Deactivate unnecessary services in the `services` file.	Chapter 2-4	Services are mapped to ports in the `services` file, which you can find in the following paths: • UNIX: `/etc/services` • Windows NT: `/winnt/system32/drivers/etc/services`
		Do you use static password files?			

Checklist 2-3 : Network Infrastructure (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-3)	Result / Comments
Network Services (continued)					
SAP Network Services					
		The following questions apply to SAP-specific network services: • What ports do you use for the various SAP network services (for example, SAPgui, message server, external RFC programs, and SAPlpd)? • Do you use the SAProuter? • Do you use Secure Network Communications (SNC)? • Is the `services` file correctly configured for your SAP-specific services?		Table 2-3-1	
Routers and Packet Filters					
		Do you use routers and packet filters? How are they configured?			
The Firewall and SAProuter					
		Is your server LAN protected with a firewall and a SAProuter?			A SAProuter alone does not protect your R/3 network.
		When using the SAProuter: • How is your configuration file (`saprouttab`) configured? Does the configuration meet your security needs? • Do you use logging? Do you use passwords?		OSS Note 30289 R/3 Online Documentation: *BC SAProuter*	You can have SAProuter activties such as connection setup and closure logged. You can also protect access to your SAProuter with a password.

Checklist 2-3 : Network Infrastructure (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-3)	Result / Comments
Secure Network Communications (SNC)					
		Do you use an external security product and SNC to provide protection between components? If yes: • Which communication paths do you protect with SNC? • What level of protection do you need for each of the various communication paths? • Is your system correctly configured to provide these levels of protection?		*SNC User's Manual* external security product documentation OSS Note 66687	

Checklist 2-4 : Operating System Protection

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-4)	Result / Comments
R/3 Security under UNIX					
Protecting Specific UNIX Properties, Files and Services					
		Do you keep your SUID/SGID programs (for example `sendmail`) up-to-date? Do you use versions in which known errors have been corrected?			
		Do you use a shadow password file? Does only the user `root` have access to it?			
		Do you use the Yellow Pages (NIS) service? Have you considered alternatives?			Before using NIS, consider the necessity of the service. There are usually alternatives available and for security reasons, we recommend that you avoid using this service.
		Do you use the Network File System (NFS) service? If yes: • Have you considered alternatives? • Is NFS only used where necessary? • Are you cautious with assigning write accesses or distributing HOME directories? • To which clients do you allow exports? Do you export to "trustworthy" clients only, and are they limited in number?			In those areas where NFS is often used (for example, for establishing a global directory for application servers or in the Transport Management System), there are often alternative solutions. Again, we recommend that you consider alternatives before deciding to use this service.
		If you use any of these services, do you restrict their use within a secure LAN?			

Checklist 2-4 : Operating System Protection (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-4)	Result / Comments
R/3 Security under UNIX (continued)					
Protecting Specific UNIX Properties, Files and Services (continued)					
		Are the users `root`, `<sid>adm`, and `<db><sid>` protected? Is `<db><sid>` locked on your application servers?			These users should also be the only users that exist on your application servers and your main instance.
		Have you protected the `.rhosts` files for these users and any other users that you consider critical?	Empty their `.rhosts` files and set the access rights to these files to '000'.		
		Have you deleted the file `/etc/hosts.equiv` or is it empty?			
		Are you up-to-date on security-related patches provided by your vendor?			
Setting Access Privileges for R/3 Under UNIX					
		How are the access rights set for SAP directories and files? Are they appropriate for your security needs?		Table 2-4-1	
		How is your UMASK defined? Is it appropriate for your security needs?			

Checklist 2-4 : Operating System Protection (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-4)	Result / Comments
R/3 Security Under Windows NT					
Windows NT Users and Groups in an R/3 Environment					
		How are your local and global groups defined? To which groups do your users and groups belong?		Table 2-4-2	For example, R/3 administrators are generally members of the global group `SAP_<SID>_GlobalAdmin` and the local group `SAP_<SID>_LocalAdmin`.
		Do you use a domain controller?			We do not recommend installing R/3 on a domain controller!
		Have you disabled the standard NT user `Administrator`? Have you created other users for administrative tasks?			
		Have you cancelled `SID<ADM>`'s membership in the groups `Administrators` or `Domain Administrators`? Do you change its password frequently? Are its rights restricted to R/3 instance-specific resources only?			
		Have you cancelled `SAPService<SID>`'s right to *Log on locally*? Are its rights restricted to R/3 instance-specific resources only? Have you restricted the user so that it cannot logon to the system interactively? Have you disabled the setting change `passwd at logon`?			

Checklist 2-4 : Operating System Protection (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-4)	Result / Comments
R/3 Security Under Windows NT (continued)					
R/3 in the Windows NT Domain Concept					
		How have you established your domain concept? Are your R/3 resources in a different domain than your Windows NT resources (for example, the domain *MASTER* for Windows NT and *SAP* for R/3 resources)?		*The R/3 Installation Guide for Windows NT.*	
		Do you use the trusted domain concept? If yes: • Have you considered alternatives? • Is the trust relationship one-way? Does only the R/3 domain *(SAP)* trust the Windows NT domain (*MASTER)* and not vice versa?			
Protecting the R/3 Resources					
		Are all your R/3 servers located in the same domain?			
		Have you cancelled `<SID>ADM`'s membership in the `Administrator` group?			
		How are the access control lists for R/3 resources defined (`\usr\sap\<sid>\...`)?			
		How are your R/3 users defined (for example: as domain users and not as local users)? How are your global and local user groups defined? How are their access rights defined? Are these definitions appropriate for your security concept?			

Checklist 2-4 : Operating System Protection (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-4)	Result / Comments
R/3 Data Security Under Windows NT (continued)					
Protecting the R/3 Resources (continued)					
		Who are your system administrators?			The standard system administrators are `<SID>ADM` and `SAPService<SID>.`
		What are the access rights for the file `sapntstartb.exe`?			Only users belonging to the local group `SAP_<SID>_LocalAdmin` should be able to use the application `sservmgr.exe` to start and stop the R/3 System. This privilege is dependent on the access rights for the file `sapntstartb.exe`.
		Can only the user who starts the R/3 System also start internal tools such as `dpmon.exe` or `gwmon.exe`?			
		Do you operate with an installation of several R/3 Systems? If yes: • Who are your administrators? • Do you administer the systems separately? • Are the systems located on a single server? • If yes: - Are the access rights for the shared memory set correctly?			We suggest *Full Control* access rights for the `SAP_<SID>_LocalAdmin` local groups for the file `saposcol.exe (`shared memory) when operating several R/3 Systems on a single server: Start `saposcol.exe` before starting R/3.

Checklist 2-4 : Operating System Protection (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-4)	Result / Comments
Logical Operating System Commands in R/3					
		Which operating system commands have you defined in R/3? Who has the authority to maintain these commands?	Transaction SM69 Authorization object: S_RZL_ADM with the value '01' in the field *Activity*.	R/3 Online Documentation: *BC Computing Center Management System → External Operating System Commands*	
		Who has the authority to execute these commands?	Transaction SM49 Authorization object: S_LOG_COM with the fields *Command*, *Opsystem*, and *Host* defined.		

Checklist 2-5 : Database Access Protection

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-5)	Result / Comments
General Recommendations					
		Have you changed the default password for SAPR3 (<SID>OFR on AS/400)?			
		Are the USR* tables protected from all access?			
		Is the T000 table protected from write access?			
		Which other tables do you consider critical and are they appropriately protected? (for example, SAPUSER, RFCDES, PA*, HCL*)			
Access Using Database Tools					
		Do you access the database using R/3 tools only? If you do use tools other than R/3 tools to access the database (for example, SQL interface or Open Database Connectivity): • Have you created specific users for this purpose? • Are their rights restricted to access rights for the necessary tables only? • Are their rights restricted to read-only access?			In regard to security, we do **not** recommend accessing the database with tools other than R/3 tools! If you do access the database with other tools, we cannot guarantee data consistency or authorization security!

Checklist 2-5 : Database Access Protection (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-5)	Result / Comments
ORACLE Under UNIX					
Changing Passwords of Database Standard Users (ORACLE / UNIX)					
		Have you changed the passwords for the standard database users?	UNIX command passwd (UP 2-5-1) svrmgrl or sqldba chdbpass (UP 2-5-2) OPS$ mechanism	Table 2-5-1	
		Do you change <sid>adm's password regularly?			
		Is the file chdbpass protected from unauthorized access?			
Protecting SAPDBA Operations (ORACLE / UNIX)					
		Do you use the expert mode for SAPDBA operations? If yes: • Is the password file passwd.dba protected from unauthorized access?			
Setting Access Privileges for Database-Related Files and Directories (ORACLE / UNIX)					
		How are the access privileges for ORACLE directories and files set? Do they meet your security requirements?	UNIX command chmod (UP 2-5-3)	Table 2-5-2	

Checklist 2-5 : Database Access Protection (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-5)	Result / Comments
ORACLE Under UNIX (continued)					
Setting Access Privileges for SAPDBA Tools (ORACLE / UNIX)					
		For ORACLE versions < 7.3: • Does `<sid>adm` belong to the UNIX group `dba`? For ORACLE versions >= 7.3: • Does `<sid>adm` belong to the UNIX group `oper`?			
ORACLE Under Windows NT					
Changing Passwords of Database Standard Users (ORACLE / Windows NT)					
		Have you changed the passwords for the standard database users?	`SVRMGR30`, `SVRMGR23`, `SQLDBA72` OPS$ mechanism (UP 2-5-7)	Table 2-5-3	
		For which users have you assigned OPS$ users? Are they limited in number?	UP 2-5-4, UP 2-5-5 and UP 2-5-6	OSS Note 50088 OSS Note 48736	
Setting Access Rights for Database-Related Files and Directories (ORACLE / Windows NT)					
		Who has access to the ORACLE files and directories?		Table 2-5-4	We suggest *Full control* access for `SAP_<SID>_LocalAdmin` and `SYSTEM` only.

Checklist 2-5 : Database Access Protection (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-5)	Result / Comments
ORACLE Under Windows NT (continued)					
Setting Access Rights for SAPDBA Tools (ORACLE / Windows NT)					
		For ORACLE versions < 7.3: • Does <SID>ADM belong to the local group ORA_<SID>_DBA? For ORACLE versions >= 7.3: • Does <SID>ADM belong to the local group ORA_<SID>_OPER?			
INFORMIX Under UNIX					
Changing Passwords of Database Standard Users (INFORMIX / UNIX)					
		Have you changed the passwords for the standard database users?	UNIX command passwd (UP 2-5-8)	Table 2-5-5	
		Have you upgraded from a release prior to 2.1J/2.2D? If yes: • Have you deleted the environment variable INFORMIX_DB_PASSWD as well as any references to it from the configuration files for <sid>adm and informix?			
Setting Access Privileges for Database-Related Files and Directories (INFORMIX / UNIX)					
		How are the access privileges for INFORMIX directories and files set? Do they meet your security requirements?	UNIX command chmod (UP 2-5-9)	Table 2-5-6	

Checklist 2-5 : Database Access Protection (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-5)	Result / Comments
ADABAS					
Changing Passwords of Database Standard Users (ADABAS / All)					
		Have you changed the passwords for the standard database users? Have you updated the `SAPUSER` table?	`CONTROL`, `XSQL` or `XQUERY` (UP 2-5-10 - UP 2-5-14)	Table 2-5-7	
Protecting CONTROL Operations (ADABAS / All)					
		Who are your CONTROL users and who are your operator users? Which tasks do each of them perform?			
Measures Specific to ADABAS under UNIX (ADABAS / UNIX)					
		Have you changed the passwords for the operating system users?	UNIX command `passwd` (UP 2-5-15)	Table 2-5-8	
		How are the access privileges for ADABAS directories and files set? Do they meet your security requirements?	UNIX command `chmod` (UP 2-5-16)	Table 2-5-9	
Measures Specific to ADABAS under Windows NT (ADABAS / Windows NT)					
		Have you changed the password for the user `<SID>ADM`?			
		How are the access rights set for the directory `%DBROOT%\config`?			We suggest *Full control* access for `Administrators` only and no access for others.
		Do you exclude access to the database with other database tools? If yes, then are the access privileges for the directory `%DBROOT%` set correctly?			We suggest *Full control* access for `Administrators` only and no access for others.

Checklist 2-5 : Database Access Protection (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-5)	Result / Comments
DB2 Common Server Under UNIX (as of Release 4.0B)					
Changing Passwords of Database Standard Users (DB2/CS / UNIX)					
		Have you changed the passwords for the standard database users?	UNIX command passwd (UP 2-5-17) DB2 control center	Table 2-5-10 R/3 Online Documentation*: BC SAP Database Administration: DB2 common server*	
		Do you occasionally change the value of the environment variable DB2DB6EKEY (or DB6EKEY, depending on release)?			If you change the value of DB2DB6EKEY, you must change it in all of the .dbenv_<hostname>.csh and .dbenv_<hostname>.sh profiles on all hosts. After changing its value, you must also change <sid>adm and sapr3's passwords.
Setting Access Privileges for Database-Related Files and Directories (DB2/CS / UNIX)					
		How are the access privileges for DB2/CS directories and files set? Do they meet your security requirements?	UNIX command chmod (UP 2-5-18)	Table 2-5-11	

Checklist 2-5 : Database Access Protection (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-5)	Result / Comments
DB2 Common Server Under Windows NT					
Assigning Users and Groups (DB2/CS / Windows NT)					
		Do your user and group assignments correspond to our standard suggestions? Do they meet your security requirements? Do your work with a domain controller? Do your user and group assignments correspond accordingly?		Table 2-5-12 Table 2-5-13	
Managing the Passwords of the Database Standard Users (DB2/CS / Windows NT)					
		Do you change the passwords for `<sid>adm` and `sapr3` regularly? Do you use the DB2 control center for this purpose?	DB2 control center	R/3 Online Documentation: *BC SAP Database Administration: DB2 common server*	Using the DB2 control center is the only way to ensure consistency. We do not recommend changing the passwords at the operating system level.
Assigning Environment Variables (DB2/CS / Windows NT)					
		Do you change the value of the environment variable `DB2DB6EKEY`? Who is allowed to change the value of this variable?	UP 2-5-20	Table 2-5-15	
Setting Access Privileges for Database-Related Files and Directories (DB2/CS / Windows NT)					
		Who has access to the DB2/CS files and directories?		Table 2-5-16	

Checklist 2-5 : Database Access Protection (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-5)	Result / Comments
DB2/400					
General Description of the DB2/400 Security Concept (DB2/400)					
		Are you familiar with the DB2/400 security concept?			
		At what level of security do you operate?	Use the WRKSYSVAL command to change the security level.		We recommend running R/3 at a security level of 40. Default=40 as of V4R2; for earlier releases, the default was 30.
Changing the Passwords for Database Standard Users (DB2/400)					
		Have you changed the passwords for the standard database users?	CHGPWD, CHGUSRPRF (UP 2-5-21)	Table 2-5-17	If you use distributed directories on multiple AS/400s over /QFileSvr.400, you must use the same passwords on all the AS/400s for each of the users (<SID>OPR, <SID>OFR, and SAP<nn>).

Checklist 2-6 : Protecting Your Productive System (Change & Transport System)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-6)	Result / Comments
The R/3 System Landscape					
		Have you separated your development, quality assurance, and productive systems?			
		Do you make changes (to include Customizing) only in the development system?			
		Do you have defined procedures for making changes and transporting them into the productive system?			
		Do you use a common transport directory for transporting changes? If yes: • Are all the systems that share the common transport directory placed in a single secure LAN?		Chapter 2-3	
		Do you have several R/3 Systems? If yes: • Are they separated into logically differentiated landscapes?			By separating the different R/3 Systems into logically differentiated landscapes, each with its own common transport directory, you can protect one system from being affected (either accidentally or on purpose) from changes made in a different system. However, how you determine which systems belong to which landscapes depends on your own priorities and infrastructure.
		Who is allowed to execute imports into the various systems?			
		Do you archive the transport information?		OSS Note 41731 or 41732	

Checklist 2-6 : Protecting Your Productive System (Change & Transport System) (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-6)	Result / Comments
The R/3 System Landscape (continued)					
		Do you use the Transport Management System (TMS): If yes: • Who is allowed to start imports? Are the authorizations correctly assigned? (System Administration authorizations) • Do you use a separate directory for the productive system? If yes, then do you transport Hot Packages into both directories?	Transaction STMS	R/3 Online Documentation: *BC Transport Management System*	TMS is available as of Release 3.1H.
Configuring the System Landscape for Changes					
		In which systems are changes required? For which objects? Are your systems correctly configured for changes?	Transactions SE03 and SE06		
Defining the Transport Process					
		How is your transport path defined? How is your transport process defined?	Either use the Transaction SE06 or TMS (as of 3.1H). You must also enter the transport path in the TPPARAM file at the operating system level.		

Checklist 2-6 : Protecting Your Productive System (Change & Transport System) (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-6)	Result / Comments
Responsibilities and their Corresponding Authorizations in R/3					
		What roles have you defined for the change and transport process? Who can perform which tasks? Are the appropriate authorizations assigned?		Table 2-6-1	
Emergency Corrections in the Productive System					
		Do you avoid making changes in your productive system?			
		Have you ensured that nobody has transport, programming, or debugging with replace authorizations in your productive system?		Table 2-6-2 OSS Note 52937 OSS Note 65968	
		Have you defined a procedure for making emergency changes in your productive system? Does this procedure ensure that all changes are supervised and double-checked?			

Checklist 2-7 : Remote Communications (RFC & CPI-C)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-7)	Result / Comments
General Security Measures					
		For which systems do you allow RFC access? Are these systems protected with the appropriate network measures (SAProuter and packet filter)?		Chapter 2-3	
		Do you include authority checks in your own function modules that can be called with RFC?			
		Who is authorized to maintain RFC destinations (Transaction SM59)? Do you keep this authorization to a minimum?	The necessary authorization objects include: • S_ADMI_FCD with the value 'NADM' • S_TCODE with the value 'SM59'		
		Do you use RFC destinations with complete logon information? If yes, • Do you store logon information for non-dialog users only? • Are their rights restricted in the target systems?	Use the program RSRFCCHK to check RFC destinations		You should only use this table to store non-dialog user information. Dialog users are prompted for their logon information at the time of connection.
		For 3.0C/D releases only: • Have you read OSS Note 43417 and taken the appropriate measures?		OSS Note 43417	

Checklist 2-7 : Remote Communications (RFC & CPI-C) (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-7)	Result / Comments
General Security Measures (continued)					
		Do you use the RFC Software Development Kit? Are you sure that it is not installed in your productive system?			
		Are external server programs defined in the `secinfo` file?	Use the program RSGWLST to check your gateways.		
		Have you disabled remote monitoring of your SAP Gateways?	Set the profile parameter `gw/monitor` to 1.	OSS Note 64016	
RFC Authorizations					
		Are you careful about assigning RFC authorizations? When assigning RFC authorizations, do you perform a trace to find out which function groups are necessary to perform an action and assign only those function groups that are necessary in the user's authorization?	The necessary authorization object for using RFC is S_RFC. UP 2-10-1 shows how to perform the trace.		In *VOLUME II*, UP 2-10-1 shows how to perform a trace for ALE applications. You can use this procedure for other RFC applications as well.
Trusted System Networks (RFC)					
		Do you use a trusted system scenario? If yes: • Do those systems in the scenario have the same security-level requirements? • Is the user administration and authorization concept identical for all systems with the trusted system scenario?			A trusted system scenario builds a single 'virtual' R/3 System. Therefore, all security requirements, user administration, and authorization concept should be the same for all systems with the trusted system scenario.

Checklist 2-7 : Remote Communications (RFC & CPI-C) (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-7)	Result / Comments
Authorizations for External Server Programs (RFC & CPI-C)					
		Which external server programs are authorized to start over the gateway? Which are authorized to register themselves on the gateway? Have you entered them in the `secinfo` file? Do you regularly maintain this file?	Use the program RSGWLST to check your gateways.	R/3 Online Documentation: *BC SAP Communication: Configuration Guide → SAP Gateway*	The path and filename for this file is defined in the profile parameter `gw/sec_info`. The default path and filename contained in the parameter is: `/usr/sap/<SID>/<instance> /data/secinfo.`
		Do you allow the execution of external operating system commands or external programs in batch jobsteps over the gateway?	Include an entry for the program `sapxpg` in the `secinfo` file.		
Secure Network Communications for Remote Communications (RFC & CPI-C)					
		Do you use Secure Network Communications (SNC) and an external security product? If yes: • Do you use SNC protection for RFC and CPI-C connections as well? Is your system properly configured?		Chapter 2-3 *SNC User's Manual*	Available for RFC and CPI-C as of Release 4.0

Checklist 2-8 : Secure Store & Forward Mechanisms (SSF) and Digital Signatures

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-8)	Result / Comments
		Are there any laws or regulations that apply to the area of application where you want to use digital signatures? What are they and do you adhere to them?			
		Do you use an external security product for Secure Store and Forward Mechanisms (SSF) in R/3?		OSS Note 86927 OSS Note 66687	SSF is available as of Release 4.0. If you do use the SSF mechanisms, then the following sections *Protecting Private Keys* and *Protecting Public Keys* apply to you.
Protecting Private Keys					
Hardware Solutions					
		Do you use smart cards for authentication purposes? Does each user have his or her own smart card?			Users should not share smart cards!
Software Solutions					
		Do you use a software solution? Is the file or directory where the user and key information is stored protected against unauthorized access?			
Protecting Public Keys					
		Do you (or your security product) use an address book to store public keys? If yes: • Is this address book protected against unauthorized access?			

Checklist 2-8 : Secure Store & Forward Mechanisms (SSF) and Digital Signatures (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-8)	Result / Comments
SAP Security Library (SAPSECULIB)					
Protecting the R/3 Application Servers' Private Key					
		Is the file `SAPSECU.pse` protected from unauthorized access?		OSS Note 110600	The file `SAPSECU.pse` is located in the `sec` subdirectory of the directory contained in the `DIR_INSTANCE` profile parameter. Normally, only `<sid>adm` has access to this file.
		Do you have reason to believe that this file has been tampered with?	Regenerate the application server's key pair by: 1. Delete the files in the `sec` directory. 2. Restart the application server.		
		Have you had to replace the R/3 application server's public key with the above mentioned procedure? Are there any applications that are using the old public key for authentication?	Re-publish the new public key to the applications that need it.		
		Do you not use digital signatures in R/3? Do you want to disable SEPSECULIB?	Replace the file `SAPSECU.pse` with an arbitrary file and restart the application server.		This is only possible if you do not use any applications that need the application's server public key.
Protecting the R/3 Application Servers' Public Keys					
		Do you use self-signed certificates or CA-signed certificates?			If you do not use an external security product, then the R/3 application server signs its own certificate.

Checklist 2-9 : Logging and Auditing

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-9)	Result / Comments
The Audit Info System (AIS)					
		Do you use the Audit Info System (AIS) on a regular basis to check and monitor your R/3 System for security issues?	Transaction SECR	OSS Note 77503 OSS Note 100609	See the OSS Notes for information on the availability of AIS.
The Security Audit Log					
		Do you use the Security Audit Log to monitor security-related events in your R/3 System? If yes: • Do you check it on a regular basis?	Use Transaction SM19 to activate the Security Audit Log and define selection criteria. Use Transaction SM20 to analyze the contents of the Security Audit Log. Use Transaction SM18 to delete old audit log files.	R/3 Online Documentation: *BC System Services → The Security Audit Log*	The Security Audit Log is available as of Release 4.0B.
The System Log					
		Do you check the System Log on a regular basis to monitor failed log-on attempts and user locks?	Transaction SM21	R/3 Online Documentation: *BC System Services → The System Log*	
Statistic Records					
		Do you use the statistic records to log user activities?	Set the profile parameter `stat/level`.		
		Do you check the statistic records when necessary?	Transaction STAT		

Checklist 2-9 : Logging and Auditing (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-9)	Result / Comments
Logging of Specific Activities					
Application Logging					
		Do you include application logging in your own developments?	Transaction SGL0		
		Do you check the application logs when necessary?	Transaction SGL1		
Workflow Execution Logging					
		Do you use the SAP Business Workflow analysis functions to monitor workflow activities?	Transactions SWI2, SWI5, etc.		
Logging Changes to Business Objects					
		Which objects do you consider critical or are susceptible to audits? Have you activated change documents for these objects?	Perform the following steps: 1. Create the change document. (Transaction SCD0) 2. Activate the change document. (Transaction SE11) 3. Generate an update for the object. (Transaction SCD0) 4. Insert the appropriate calls in the corresponding programs.		

Checklist 2-9 : Logging and Auditing (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-9)	Result / Comments
Logging of Specific Activities (continued)					
Logging Changes to Table Data					
		Which tables to you consider critical or susceptible to audits? Have you activated table recording in general? Have you activated table recording for those tables you want to have logged?	Perform the following: 1. Set the `rec/client` profile parameter. 2. Set the *Log data changes* flag for those tables you want to have logged.	OSS Note 1916 OSS Note 112388	
Logging Changes to User Master Records, Profiles, and Authorizations					
		Do you regularly check changes to user master records, profiles, and authorizations?	Authorization Infosystem or Transaction SU01.		

Checklist 2-10 : Special Topics

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-10)	Result / Comments
R/3 Internet Application Components (IAC)					
The Overall Architecture of the ITS					
		Do you use Internet Application Components?			
		Are your AGate and WGate located on separate machines?			
A Secure Network Infrastructure for the ITS					
		How is your network infrastructure set up? Where have you included packet filters and routers in your infrastructure?		Chapter 2-3	
		Do you use a separate system (replicated with ALE) instead of your productive system for your Internet system?			
Configuring the Server and Network Components					
Protecting the Web Server					
		What types of communication protocols do you require (for example, HTTP, HTTPS)? How is your Web server configured? Have you configured it to only allow those communication protocols that you require?		Chapter 2-3 Chapter 2-4	
		Is your Web server (where the WGate is located) isolated from your corporate network?			

Checklist 2-10 : Special Topics (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-10)	Result / Comments
R/3 Internet Application Components (IAC) (continued)					
Configuring the Server and Network Components (continued)					
Protecting the AGate Server					
		Where is your AGate located? Is it protected from the external network with a firewall and SAProuter?		Chapter 2-3	We suggest placing your AGate within your internal network.
		How are the TCP ports for ITS (`sapavx<xx>_<INST>`) in the file `/etc/services` defined?			
		Are the port assignments identical for the WGate and AGate hosts?			
		Do you use the SAProuter to control the connection between the WGate and the AGate? How is your SAProuter configured for WGate←→AGate communications? Do the Windows NT registry entries on the WGate host correspond correctly?			
		Do you use other commercial firewall products to relay the TCP connection from the WGate to the AGate? Do the Windows NT registry entries on the WGate host correct?			

Checklist 2-10 : Special Topics (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-10)	Result / Comments
R/3 Internet Application Components (IAC) (continued)					
Configuring the Server and Network Components (continued)					
Protecting the R/3 Servers					
		Do you provide additional protection between the AGate and the R/3 application server? (Do you have a firewall between the AGate and the application server?)		OSS Note 104576	
Using Security Services / Providing Privacy					
Between the Web Browser and Web Server					
		Do you offer your services to external users, or only to internal users?			
		Do you use HTTPS and X.509 certificates for communication between the Web browser and server? Do you have an established corporate Certificate Authority (CA) or do you use an external CA?			
		How is your Web server configured? Is it configured to only allow connection requests that present valid browser certificates? Which browser certificates do you accept?			
Between WGate and AGate					
		As of ITS 2.0: • Do you use Secure Network Communications (SNC) to provide encryption for the connection between the WGate and AGate?		Chapter 2-3	

Checklist 2-10 : Special Topics (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-10)	Result / Comments
R/3 Internet Application Components (IAC) (continued)					
Using Security Services / Providing Privacy (continued)					
Between AGate and R/3					
		As of ITS 2.2: • Do you use Secure Network Communications (SNC) to provide encryption for the connection between the AGate and R/3?			
Authenticating Users					
		Do you have services users that are worth protecting? If yes: • Is the AGate protected from unauthorized access?			
Protecting Session Integrity					
		Do you have an Internet or an Intranet infrastructure? Do you use proxys and load balancing? To what degree do you need to compare and verify IP addresses? How is the following registry key defined? • `HKEY_LOCAL_MACHINE\SOFTWARE\SAP\ITS\2.0\<INST>\Connects\IPChecking`			The default value is 255.255.255.255 which specifies that the entire IP address is compared. For example, a value of 255.255.0.0 specifies that only the leading figures of the address should be compared.
Setting Security Levels					
		At what security level do you operate your ITS (1,2,or 3)?	To change the security level, use the command-line utility `itsvprotect`.		

Checklist 2-10 : Special Topics (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-10)	Result / Comments
R/3 Internet Application Components (IAC) (continued)					
Declaring Allowed Applications					
		Do you use transactional IACs?	Define a service file for the transaction.		You can only use transactions that have a corresponding service file. Defining a service file is part of the process of creating the transaction.
		If you use WebRFC or WebReporting and have a release as of Release 4.5: • Have you explicitly released those Reports, Reporting trees and Function Modules that are accessible over the Internet?	Transaction SMW0		
		If you use WebRFC or WebReporting and have Release 3.1H: • Have you ran the available patch to prevent the starting of reports that contain an empty authorization group?		OSS Note 92725	
		If you do not use WebRFC or WebReporting, then do you want to disable the use of WebRFC?	Delete the file `SAPXGWFC.dll`.		
Protecting Application Link Enabling (ALE) Applications					
		Do you use ALE applications?			
		How are your ALE users set-up? What roles do you have and who has which authorizations?	Transaction SALE		
		Where are your users and passwords stored? Is this information protected from unauthorized access?	system-dependent		ALE users and passwords are generally stored outside of the R/3 System.

Checklist 2-10 : Special Topics (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-10)	Result / Comments
Protecting Application Link Enabling (ALE) Applications (continued)					
		Is your distribution model protected from unauthorized access?	The authorization object needed to maintain the distribution model is B_ALE_MODL.		
		Are authorizations in the target system for ALE users kept to a minimum?			
		Do you set up special users for ALE? Do they have only ALE authorizations?			
		Do you avoid giving ALE authorizations to other users?			
		Are your ALE users in the target system type CPIC?			
		Do you use background processing, or immediate processing?			
		For background processing: • What authorizations do your ALE users have? Do you avoid giving them authorizations for the receiving application?			
		For immediate processing: • What authorizations do your ALE users have? Are they restricted to only those application authorizations that they need?	Authorization trace (UP 2-10-1)		

Checklist 2-10 : Special Topics (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-10)	Result / Comments
R/3 Online Services					
		Are you aware of the security measures that we take at SAP? Do you take those measures that we recommend?		OSS Note 35010 OSS Note 46902 OSS Note 35493	
		Do you use a hardware router for the connection? Do you restrict access authorizations for the router?			
		Do you use the SAProuter program? Do you use and check the SAProuter logs? Do you use password protected connections?			
		Do you use separate users for online services? Are they tailored to the type of service required? Are they set-up in test clients?			
		Do you monitor the activities and/or check them after a session is completed?	Transaction STAT		
		Do you protect your users' passwords?	Use a separate channel (telephone or separate document) to disclose passwords.		Do not disclose users' passwords over the remote connection!
		If you do have to allow access over the user `<sid>adm`, do you change its password immediately afterwards?			
		Do you deactivate users and passwords after a session is terminated?			
		Do you deactivate the remote connection and close the OSS connection after task completion?			
		Do you set time limits for OSS connections?			

Checklist 2-10 : Special Topics (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-10)	Result / Comments
Virus Protection and Integrity Checks					
		Do you use virus checkers? Do you keep them up-to-date? Are your users informed of the dangers of viruses and using unchecked programs?			
Protecting Specific Tables, Authorization Objects, etc.					
SAP_ALL Authorization					
		Have you distributed the authorizations from SAP_ALL among various users? Does only one user have the SAP_ALL authorization? Is this user's password kept secret and in a safe place? Do you save this user only for emergencies?			
SAP_NEW Authorization					
		Do you have a long list of SAP_NEW profiles?	Review and re-establish your authorization concept.		
		Do you "clean-up" your SAP_NEW profiles after an upgrade? Have you distributed the profiles contained in the SAP_NEW_* profiles? Have you maintained their values? Have you deleted the SAP_NEW_* profiles after distributing and maintaining them?	Perform the following steps: 1. Delete SAP_NEW_* profiles that you do not need to distribute. (The profiles are already distributed.) 2. Distribute the rest of the SAP_NEW_* profiles and maintain their values. 3. Delete the profile SAP_NEW.		

Checklist 2-10 : Special Topics (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-10)	Result / Comments
Protecting Specific Tables, Authorization Objects, etc. (continued)					
Table T000					
		Do only system administrators have maintenance access for Table T000?	The necessary authorization object is S_ADMI_FCD.		
		Do you have a defined process for creating and maintaining clients?			
		Does the S_TCODE authorization object contain the table and client maintenance transactions SCC4, SM30 and SM31?			
		Are the fields in the authorization object S_TABU_DIS set as indicated below? • **Field:** *Activity*; Values: `02`, `03` • **Field:** *Authorization group*; Value: SS			
		Is the indicator for client-independent maintenance field for the authorization object S_TABU_CLI set to the value 'X'?			
HR Tables					
		For Releases 3.0A-C: • Have you explicitly assigned HR tables to the authorization group PA? • Have you excluded the group PA from the authorization object S_TABU_DIS?			

Checklist 2-10 : Special Topics (continued)

Nr.	Prio.	Security Item	Method	Reference (VOL.II, Ch. 2-10)	Result / Comments
Protecting Specific Tables, Authorization Objects, etc. (continued)					
HR Authorization Profile P_BAS_ALL					
		Are all your HR tables assigned to either the PC or PS table classes? Have your restricted the *Authorization group* field in P_BAS_ALL to PC and PS?		OSS Note 11796	
System Profile Parameter Files					
		Are the system profile parameter files <SID>_<Instance>, START_<Instance>, and DEFAULT.PFL, protected form unauthorized access? Do you regularly check their authenticity?			

Index

R/3 Security Guide / Feedback Reply Form

To:

SAP AG
CCMS & Security Department
Postfach 1461
D-69190 Walldorf
Germany

Fax: **+49-6227 / 7-41198**

From:

Name: ....

Position: ....

Dept.: ....

Company: ....

Address: ....

....

Telephone: .... Fax: ....

email: ....

Subject: Feedback to the R/3 Security Guide

Feedback applies to: R/3 Security Guide, Volume .... Version .... Chapter ....

R/3 Release .... Database: .... Operating System ....

Were you able to find the information you needed in the guide?

○ Yes

○ No

How well does the R/3 Security Guide meet your needs?

○ Very well

○ Well

○ Not very well

○ Not at all

Why or why not?
(Use space below.)

Are you?

○ Requesting further information

○ Reporting additional information

○ Reporting missing information

○ Reporting an error

○ Other

Feedback (use additional pages if necessary):

....

....

....

....

....

....

....

....

....

....

....

Thank you for your information.