# Contents

Objective........................................................................................................................................... 3  
Methodology...................................................................................................................................... 4  

Phase 1: User Authentication........................................................................................................... 4  
  User Accounts.................................................................................................................................. 4  
  Password Security............................................................................................................................ 4  
  Default Accounts ............................................................................................................................. 5  
  Session Security ............................................................................................................................... 6  

Phase 2: User Authorization................................................................................................................ 7  
  Authority Checks.............................................................................................................................. 7  
  Profile Generator .............................................................................................................................. 7  
  Authorization Infosystem .................................................................................................................. 7  
  Specific Authorization Checks ......................................................................................................... 8  

Phase 3: Network Communications .................................................................................................. 12  
  Standard Network Configuration Security ....................................................................................... 12  
  SAPRouter ....................................................................................................................................... 13  
  Secure Network Communications (SNC)........................................................................................ 15  

Phase 4: Auditing and Logging ........................................................................................................... 16  

Phase 5: Database Security ................................................................................................................ 17
Objective

This paper describes a security assessment framework for SAP R/3 implementations. It covers various aspects not just of the SAP system itself, but also the security issues of the database and underlying operating system that are in relation to SAP. The topics covered here include authentication, authorization, logging and auditing, secure store and forward mechanisms, remote communications, the R/3 change and transport system, and the network architecture to be adopted.

The key assumptions made herein are that the reader is conversant with SAP R/3 administration, and that there exists an Organizational Security Policy (OSP). Also, the actual implementation of security within your SAP R/3 system is specific to each organization. Therefore, this exercise, just as any other security exercise, must be preceded by a structured and process-based risk assessment exercise. The results from the risk assessment exercise will help define the appropriate security posture to be adopted.
Methodology

The methodology to be adopted for the security assessment of a SAP R/3 implementation are illustrated below. Each section of security is explained in the ensuing paragraphs.

Phase 1: User Authentication

User Accounts
The main aspect of user authentication for a SAP installation is auditing the user accounts created. Here we need to check the following:

1. Listing of all user accounts present on the system
2. Any vendor or generic accounts created, other than the default SAP accounts (more on this later)
3. Accounts of users who have left the organization or are on leave, and need to be disabled (as per the Security Policy)
4. Last successful and unsuccessful logins for all users (report RSUSR006 and Security Audit Log Transactions SM18, SM19 and SM20)

Password Complexity
The next step is to check for password strength parameters being enforced for the SAP users. R/3 provides a number of password complexity enforcement rules, such as a minimum password length of 3 (and strangely a maximum password length of 8), first three characters cannot be the same, first three characters cannot appear in the same order as the username, last five passwords cannot be reused, etc.

Administrators can also define their own security checks for user passwords in the customer exit SUSR001. Here we will check whether standard complexity measures such as disallowing the use of dictionary words, ensuring there is a mix of alphanumeric and punctuation mark characters, and that the administrator password is of the maximum allowable length of 8 characters and is sufficiently complex. Administrators can also specify impermissible passwords in the Table USR40 (using the Transaction SM30).
Furthermore, ‘profile parameters’ can also be defined to influence the choosing of strong passwords. These parameters are:

- **login/min_password_lng**: Minimum length 3. Suggested value is 6 or as per OSP\(^1\).
- **login/password_expiration_time**: Number of days after which a password must be changed. Default value is 0 (no limit). Suggested value is: 40 (days) or as per the OSP.

**Default Accounts**

As is the case with many other systems, SAP R/3 creates a number of default accounts, which merit special attention.

<table>
<thead>
<tr>
<th>Username</th>
<th>Description</th>
<th>Clients</th>
<th>Default Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP*</td>
<td>This is the SAP R/3 Super-user account</td>
<td>000, 001, 066 (as of Release 3.0D) all new clients</td>
<td>06071992 PASS</td>
</tr>
<tr>
<td>DDIC</td>
<td>ABAP Dictionary and software logistics super user</td>
<td>000, 001</td>
<td>19920706</td>
</tr>
<tr>
<td>SAPCPIC</td>
<td>CPI-C user for the R/3 system</td>
<td>000, 001</td>
<td>admin</td>
</tr>
<tr>
<td>EARLYWATCH</td>
<td>Interactive user for the Early Watch service in client 066</td>
<td>066</td>
<td>support</td>
</tr>
</tbody>
</table>

Table 1: Default SAP R/3 Account Credentials

It is not possible to delete the SAP* user. The suggested measure is to create a new super-user account with a complex password, and **deactivate** the SAP* default account. This can be done by activating the profile parameter **login/no_automatic_user_sap** or **login/no_automatic_user_sapstar**. Even though the SAP* account is being deactivated, the default password for this account must be changed.

As for the DDIC user, this account cannot be deleted or deactivated either. And therefore, the best protection is to change its default password.

The SAPCPIC user can be either disable or its default password can be changed. Either method involves disabling certain functionality. Therefore, this is an organization-specific issue where the functionality required will decide which method is best.

---

\(^1\) Organizational Security Policy
The EARLYWATCH account is used specifically for the Early Watch™ service, and its password must be changed, and the account locked out. It should be unlocked when required, and re-locked after use.

Session Security
SAP R/3 provides various mechanisms to control user sessions. Some of these are:

- Listing out user logins and logout and the terminals from where the authentication attempts took place, as well as information whether the logins were successful or not. This can be done using the Security Audit Log (Transactions SM18, SM19 and SM20).

- Terminating a logged in user’s session after a specific number of unsuccessful logins using the profile parameter login/fails_to_session_end.

- Logging off users after a specific period of inactivity by setting the profile parameter rdisp/gui_auto_logout.

- Locking a user account after a specific number of failed authentication attempts with that user account, by setting the profile parameter login/fails_to_user_lock.

- When a user logs in he can access information about the last login time and date and verify whether this is correct.

- The SAP Logon Pad, which ensures that the users cannot change the SAP Logon configuration.

Session security measures must also deal with SAP Shortcuts, which are used to store the user’s logon information on the client. Although this is a convenience measure, the authentication data is saved in plain text. The use of SAP Shortcuts should therefore be discouraged, or administratively prohibited.
Phase 2: User Authorization
Since the SAP R/3 system is used for mission critical processes, it is extremely essential to design and implement a structured authentication matrix. By default, R/3 does not allow a user to execute any transactions or programs unless she has been explicitly authorized to do so. Authority checks must be used to grant users specific authorization to carry out their functions.

Defining such an authorization matrix requires careful thought and planning. SAP R/3 provides a number of useful features to implement this.

Authority Checks
R/3 enforces the authorization concept by performing authority checks. These authority checks make sure that the user has the appropriate authorizations in her master record before allowing her to perform any actions. The four types of authority checks are:

- **R/3 Start Transaction Authorization**: The authorization given to the user to start menu-based or command-line transactions.

- **Transaction-specific Authorization**: Besides the authority to start transactions, the users can also be required to possess additional authorizations to successfully complete the transaction.

- **AUTHORITY-CHECK at program level**: SAP programs include an AUTHORITY-CHECK at the code level itself. Custom-developed transactions can also be protected with this mechanism.

- **Report Classes and Table Authorization Groups**: In addition to the above authorizations, reports can be assigned to report classes and authorization groups can be assigned to tables.

Profile Generator
SAP R/3 provides a tool to make assignment of user authorization easier, called as the Profile Generator. Here, we would check if the organization has utilized the Profile Generator to implement its authorization matrix. If so, then the following needs to be assessed:

- Which transactions have been assigned to which job roles?

- Which activity groups have been created for each of the job roles?

- What authorization profiles have been created and assigned to each activity group?

- Which activity groups have been assigned to which agents? Note: agents need not be R/3 users, and can include Jobs, Positions and Organizational Units as well.

Authorization Infosystem
The next step would be to obtain a report of the complete authorization matrix as it exists within the SAP R/3 system. This can be done using the Authorization Infosystem, to obtain the following views:

- Users with certain authorizations

- All users with a given authorization
Specific Authorization Checks
Besides gaining an authorization overview, we would determine the following specific authorizations:

1. Determine who has the capability to add user master records.
   S_USER_GRP and S_USER_ALL
2. Determine who can maintain profiles.
   S_USER_PRO
3. Determine who can maintain authorizations.
   S_USER_AUT
4. List all SAP supplied profiles and authorizations that have been modified and review for completeness.
5. List of the system parameter file (RSPARAM) and review the authentication controls
   - login/min_password_lng
   - login/password_expiration_time
   - login/fails_to_session_end
   - login/fails_to_user_lock
6. Determine how the profile SAP_NEW is being used.
7. Review SAP for any new objects/values that have been defined
8. Review changes to table AUTH for new fields and table TOBJ for new objects
9. Determine if all users have been assigned to a group. (Table USR02)
10. Determine that the SAP* profile has a user master record and that SAP* has had its password changed and added to the SUPER group. Also determine if the password has been stored in a secured location in case of an emergency.
11. Determine who are the members of the SUPER group and ensure that their membership is required.
12. Determine how many users have SAP_ALL access in the production environment. List all users with the following standard system profiles:
   - SAP_ALL: All R/3 privileges
   - S_A.SYSTEM: All SAP system functions
   - S_A.ADMIN: System administration
   - S_A.CUSTOMIZ: SAP customizing system
   - S_A.DEVELOP: SAP development environment
   - S_ABAP_ALL: All authorizations for ABAPs

   TOOLS>ADMINISTRATION>USER MAINTENANCE>USERS>MAINTAIN
   USERS>INFORMATION>OVERVIEW>USERS> profile name >LIST>PRINT

13. List all users with special SAP system administration
   - S_ADMI_FCD: Access to ABAP/4 Data Dictionary
   - S_BDC_ALL: Batch Input
   - S_DDIC_ALLDYNPRO and ABAP/4
   - S_EDI_BUK: Creating/modify ABAP/4 programs and use of screen painter
   - S_EDITOR: Ability to edit and modify ABAP’s programs
   - S_PROG_ADM: Running ABAP/4 programs and submitting background processing
   - S_PROGRAM: Ability to run ABAPs
   - S_TABU_ADM: System Table – table maintenance
   - S_BTCH_ADMS_ENQ_ALL: Background Processing
   - S_TSKH_ADMS_ENQ_ALL: Transactions – lock management for processing

14. Determine who has access to the ABAP/4 Data Dictionary
   - For this object list users that have the following values:
     - REPL, SE01 (CTS requests) and/or DDIC in the System Administration Function field
     - SM21 in the Field Administration Function field (allows access to the system log)
     - TCOD which allows the user to change additional authorization checks

   Versions for a particular object are maintained as: Utilities>Version Management Menu.

   Temp
Use Transactions:
- SE16 Data Browser
- SE12 Dictionary Display
- SE80 Object Browser
- SCU3 Table history transaction

15. Determine who has batch access
   - S_BDC_MONI
   - S_BDC_ALL
   - S_BTCH_ADM
   - S_BTCH_ALL
   - S_BTCH_USR

   Batch log files (bdc/logfile) should be reviewed and any deletions, modifications, or abended sessions subject to investigation and should be secured through the correct use of the operating system security.

16. List users with authorization for SM04, SM50 (S_TSKH_ADM) which grants access to the transaction locking function. Determine which transactions are locked on the production system by viewing additional authority checks in table TSTC (Tools>Administration>Tcode Administration). Ensure that at a minimum the following transactions are locked:
   - SE01 Correction and transports
   - SE38 Ability to execute ABAP programs
   - SE11 Maintain data dictionary objects

17. Determine if the parameters for the trace and log files are adequate
   With the RSPARAM report, review the rstr/* and rslg/* parameters

   If a transaction cannot finish correctly, the system rolls it back. The dialog program first generates a log record in the VBLOG table.

   Transaction SM21 or Tools>Administration>Monitoring>System Log
Selection Criteria:

Date/Time – To – Date/Time

By User, Trans Code, SAP Process, Problem Classes (Messages)

18. Determine if Spool access is properly restricted.
   Verify who has the authorization object S_ADMI_FCD, S_SPO_ACT, and S_SPO_DEV

19. Is access to the SAP archiving function restricted? (Verify which profiles have access to transaction F040).

20. Determine who has access to the SAP customizing system (IMG, menu customizing)
   S_A.CUSTOMIZ  The profile gives all authorizations required for the Basis activities in the customizing menu. (Table USR10 gives an overview of all authorization objects in a profile.)
Phase 3: Network Communications

Network level security is as important as securing the SAP configuration, the operating systems and the database. Securing your SAP network requires careful planning in order to decide placement of components and configuration of access control lists on firewalls and/or routers.

Here there are two options available:

- Standard network configuration security
- Use of the SAPRouter

Standard Network Configuration Security

The suggested network architecture for a secured SAP system is to put the SAP application server and the database server in a separate segment. This segment must be protected from the SAP users as well others, as shown below:

As per SAP R/3 guidelines, specific ports need to be opened up between the SAP front-end and the SAP application servers. It is also strongly recommended to completely block access from the SAP front-ends to the Database server. This is easier if the application and database servers are on separate systems. However, in the case of smaller organizations, this may not be possible. Under these circumstances, the Oracle or DB2 database ports must be disallowed access from IP addresses other than those belonging to the management workstations.
The following port configurations must be implemented:

<table>
<thead>
<tr>
<th>Connection</th>
<th>Symbolic Port Name</th>
<th>Direction of Information</th>
<th>Example: &lt;nn&gt;= 01</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAPgui – Application Server (dispatcher)</td>
<td>sapdp&lt;nn&gt;2</td>
<td>-&gt; (out-in)</td>
<td>3201</td>
</tr>
<tr>
<td>SAPgui – Message Server (load-balancing)</td>
<td>Sapms&lt;sid&gt;</td>
<td>-&gt; (out-in)</td>
<td>3600</td>
</tr>
<tr>
<td>External RFC client – Application Server (gateway)</td>
<td>Sapgw&lt;nn&gt;</td>
<td>-&gt; (out-in)</td>
<td>3301</td>
</tr>
<tr>
<td>RFC Server – Application Server</td>
<td>Sapgw&lt;nn&gt;</td>
<td>&lt;-- (in-out)</td>
<td>3301</td>
</tr>
<tr>
<td>Application Server - SAPIpd</td>
<td>Printer</td>
<td>-&gt; (out-in)</td>
<td>515</td>
</tr>
<tr>
<td>Anyone – SAPRouter</td>
<td>Sapdp99</td>
<td>-&gt; (out-in)</td>
<td>3299</td>
</tr>
</tbody>
</table>

Table 2: SAP R/3 Components and Required Ports

**SAPRouter**

The SAPRouter is a software program developed by SAP to transport R/3 connections across firewalls. The SAPRouter is a proxy at the NI layer (Network Interface - NI is SAP’s abstract network protocol based on TCP/IP). In addition, it implements the logging of connections at various levels of detail.

Note: The SAPRouter is not intended as a replacement to a firewall, but rather as a proxying device, which works in conjunction with a well-configured firewall.

With the SAPRouter in place, we need to check if the following suggested network architecture is in place:
If the SAPRouter is being used, we need to check whether it has been configured securely or not. This includes verifying:

- The IP addresses allowed connection to the various SAP R/3 components.
- The logging and auditing levels configured within the SAPRouter
- Administration access to the SAPRouter
- SAPRouter - SAPRouter communication implemented within a WAN
Secure Network Communications (SNC)
SNC is a software layer in the R/3 architecture that provides an interface to an external security product. With SNC, you can strengthen the security of your R/3 System by implementing additional security functions that R/3 does not directly provide (for example, the use of smart cards for user authentication). SNC provides security at the application level. This means that a secure connection between the components of an R/3 System (for example, between SAPgui and the R/3 application server) is guaranteed, regardless of the communication link or transport medium.

Note: SNC cannot be implemented between the SAP Application Servers and the SAP Database. Thus, it is strongly recommended to put the SAP Application and Database Servers in the same network segmented protected from the other components and SAP front-ends.

If SNC is implemented (and this is strongly recommended), we need to check at which of the following layers it has been implemented:

1. **Authentication only**: Only the data transmitted during the authentication process is protected. This is the minimum level that must be implemented.
2. **Integrity Protection**: This level protects unauthorized changes to the data as it is being transmitted between the sender and the receiver
3. **Privacy Protection**: This is the maximum protection level possible, and it encrypts all the messages. It includes the above two layers.
Phase 4: Auditing and Logging

R/3 keeps a variety of logs for system administration, monitoring, problem solving, and auditing purposes. Logs and audits are important for monitoring the security of your system and to track events in case of problems.

Here we will mainly use the Audit Infosystem (AIS) to analyze security aspects of the R/3 system in detail. We will check for the following:

- Successful and failed user logons are being logged
- Successful or failed RFC logon attempts
- RFC calls to function modules
- Changes to User Master Records
- Successful and failed transaction starts
- Changes to the audit configuration itself

The following profile parameters influence the audit logs:

<table>
<thead>
<tr>
<th>Profile Parameter</th>
<th>Definition</th>
<th>Standard or Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsau/enable</td>
<td>Activates the audit log on an application server</td>
<td>0 (audit log is disabled)</td>
</tr>
<tr>
<td>rsau/local/file</td>
<td>Specifies the location of the audit log on the application server</td>
<td>Standard Value: /usr/sap/&lt;SID&gt;/&lt;instno&gt;/log/audit_&lt;SAP_instance_number&gt;</td>
</tr>
<tr>
<td>rsau/max_diskspace_local</td>
<td>Specifies the maximum length of the audit log</td>
<td>1,000,000 bytes</td>
</tr>
<tr>
<td>rsau/selection_slots</td>
<td>Specifies the number of selection slots for the audit</td>
<td>2</td>
</tr>
</tbody>
</table>

The other aspects of logging that need to be reviewed are:

- **Application logging**: Whether it is possible to reconstruct the execution of an application
- **Workflow Execution logging**: Whether the SAP Business Workflow is being used to audit transactions across various applications
- **Change Document Logging**: SAP R/3 provides a mechanism to maintain an audit trail for changes made to critical documents.
- **Changes to Table Data**: As with business objects, critical tables containing sensitive data must also have an audit trail enabled to track changes
- **Changes to User Master Records, Profiles and Authorizations**: Changes to a user’s authorization, her password, user type, user’s profile, group, etc. can also be logged
Phase 5: Database Security

The key measures that must be implemented for the security of the Oracle database being used by SAP R/3 are as follows:

- Only R/3 tools (such as SAPDBA) must be used to access the database
- The initial password for the SAPR3 user must be changed
- Access to USR* tables must be prohibited
- Write access to T000 table must be prohibited
- Application specific tables must be protected in accordance with the authorization matrix defined earlier

In some situations, we have observed that applications are written to directly access the database using the R/3 SQL interface or ODBC connectivity. This must be strongly recommended against. However, if you have legacy applications that work this way, the following must be taken into consideration:

- The application must not use the SAPR3 account to connect to the backend database
- The access rights for the application account must be restricted only to the necessary tables
- SAP does not guarantee data consistency and integrity if user applications bypass R/3 tools to access the database directly

For other Oracle security measures, read an article written by our team on “Oracle Security and Auditing” at IT Audit.