Contributed March 22, 2001

TIER I AUDIT GUIDE

Security

Audit: **SAP Pre-Implementation Audit** **Ref.:** **K-1**

Period: **1997**

TESTING OBJECTIVE
Security Access to the SAP R/3 application and it's database is properly restricted.

BUSINESS EXPOSURES AND EXPECTED CONTROLS / PROCEDURES	Y ☑ **Describe ACTUAL CONTROLS / PROCEDURES** OR N ☑ **Describe EXPOSURE OR MITIGATING CONDITION**
Access to application functions are not authorized (SAP R/3)	Control Y ☐ N ☐ Audit Test No:
?? System security file parameters (e.g. password length/format, forced password sessions, user failures to end session etc.) have been set to ensure confidentiality and integrity of password. ?? Set up modification of user master records follows a specific procedure and is properly approved by management. ?? Set up and modification of authorizations and profiles follows a specific procedure and is performed by somebody independent of the person responsible for user master record maintenance. ?? An appropriate naming convention for profiles, authorizations, and authorization objects has been developed to help security maintenance and to comply with required SAP naming conventions. ?? A user master records is created for each user defining a user ID and password. Each user is assigned to a user group , in the user master record, commensurate with their job responsibilities. ?? Check objects have been assigned to key transactions (through table TSTC) to restrict access to those transaction. ?? Authorization objects and authorizations have been assigned to users based on their job responsibilities. ?? Authorization objects and authorizations have been assigned t users ensuring segregation of duties. ?? Users can only maintain system tables commensurate with their job responsibilities. ?? All in house developed programs contain authority Check statements to ensure that access to the programs are properly secure.	

Contributed March 22, 2001

TIER I AUDIT GUIDE

Security

Audit: **SAP Pre-Implementation Audit** **Ref.:** **K-2**

Period: **1997**

TESTING OBJECTIVE
Security Access to the SAP R/3 application and it’s database is properly restricted.

Contributed March 22, 2001

TIER I AUDIT GUIDE

Security

Audit: **SAP Pre-Implementation Audit** **Ref.:** **K-3**

Period: **1997**

TESTING OBJECTIVE

Security
Access to the SAP R/3 application and it's database is properly restricted.

Application Security

1. Verify that security parameters are reasonable. The parameters (including those shown below) are setup at system start up and can be viewed using the report RSPARM (instance Specific) and RSPARM1 (Default settings) or though transaction TU02.

?? Login/min_password_lng- Minimum password length
?? Login/passowrd_expiration_time _number of days after which a password must be changed.
?? Login/fails_to_session_end- number of times a user can enter an incorrect password before the system ends the Login attempt.
?? Lgin/fails_to_user_lock- Number of times a user can enter an incorrect password before the system locks the user against future logon attempts. Passwords are automatically unlocked at the start of the next day. Therefore passwords are locks should be investigated by a security admin. Prior to re start of the machine.

2. Select a sample of …… Changes to User Master records, profiles and Authorizations and ensure the changes were properly approved. (The changes can be viewed by transactions SU91, and Su93 and are logged in tables USH02, USH04, USH10, and USH12.)
3. Ensure that security administration is properly segregation . At a minimum there should be separate administrators responsible for:

?? User master maintenance (this process can be further segregated by user group.)
?? User profile development and profile activation (these processes can be further segregated.)

4. Verify that a naming convention has been developed for profiles, authorizations and in-house developed authorization objects to ensure

?? They can be easily managed.
?? They will not be overwritten by a subsequent release upgrade (for Release 2.2 should begin with Y_ or Z_ and for Release 3.0 by Z_ only.)

5. Assess through audit software, Through transaction Su45 or through a review of table USR02, whether user master records have been properly established and in particular:
?? Each user is assigned to a unique user master record, counting a used and password, in order to gain access o the system.
?? Each user is assigned to a user group commensurate with their job responsibilities.
?? The SAP* user master record has no assigned profiles or authorizations and has been assigned to the user group Super (in the user master record.) Only the designated super user is assigned to this user group.
?? Validity periods are set for user master records assigned to temporary staff.

6. Assess, through audit software or through transaction Su44 or SU60, that standard or modified SAP profiles and authorizations are assigned to users only after the associated authorization object and authorization field values have been reviewed to ensure they are commensurate with the users job responsibilities, and that segregation of duties is maintained (refer to attached appendix for a listing of authorization objects and possible value sets.) Also ensure that:

?? The SAP* profile is not assigned to any user master records.
?? The SAP_NEW profile is not signed to any user master records. Verify that procedures exist for assigning new authorization objects form this profile, to users, following installation of new SAP releases.

7. Assess through audit software or through a review of table TSTC or TSTCA that check objects have been properly assigned to restrict access to key transactions.
8. Assess through audit software or a review of the use of the authorization object S_TABU_DIS (through transaction SU44 or SU60) and review of table authorization classes (TDDAT) whether:

?? All system tables are assigned an appropriate authorization class.
?? Users are assigned system table maintenance access (Through S_TABU_DIS) based on authorization classes commensurate with their job responsibilities.

Contributed March 22, 2001

TIER I AUDIT GUIDE

Security

Audit: **SAP Pre-Implementation Audit** **Ref.:** **K-4**

Period: **1997**

TESTING OBJECTIVE
Security Access to the SAP R/3 application and it’s database is properly restricted.

Perf. By

Contributed March 22, 2001

TIER I AUDIT GUIDE

Security

Audit: **SAP Pre-Implementation Audit** **Ref.:** **K-5**

Period: **1997**

TESTING OBJECTIVE

Security
Access to the SAP R/3 application and it's database is properly restricted.

9. Asses through audit software or a review of the use of the authorization objects S_Program and S_Editor (through use of SU44 or SU60) and the review of program classes (TRDIR) whether:
   - ?? All programs are assigned the appropriate program class.
   - ?? Users are assigned program classes commensurate with their job responsibilities.

10. Ensure through a review aof a sample of …… In-house developed programs that the progrma code either:

   - ?? Contains an Authority-Chek statemnt referring to an appropriate authorization onject and vale set values; or

   - ?? Contains a progrma Include statement , where the referred progrma contains an Authority-Check statement referring to an appropriate authorization object and value set values.

Contributed March 22, 2001

TIER I AUDIT GUIDE

Security

Audit: **SAP Pre-Implementation Audit** **Ref.:** **K-6**

Period: **1997**

TESTING OBJECTIVE

Security
Access to the SAP R/3 application and it's database is properly restricted.

CONCLUSION

	YES	NO
Controls and procedures are in place and operating effectively to meet the Testing Objective. If no, please explain briefly:		

Additional Testing required? YES ☐ NO ☐ Mgr. Approval: _____ Date: _____