SAP ECC Audit Guidelines

Applies to:

Applies to SAP R/3 and ECC systems. For more information, visit the Security homepage.

Summary

The Purpose of this document is to provide the Security Administrator with guidance on preparing for the SAP System Audit. This will also help the Security Administrator in keeping the system complaint and secure.

Author: Nishant Sourabh

Company: IBM

Created on: 30 December 2009

Author Bio

Nishant Sourabh is SAP Certified Security Consultant and is working in the area of SAP Security for more than 4 years. He is presently with IBM India and has worked on SAP R/3, ECC, BW, CRM and APO modules.

Table of Contents

Scope

The Scope of this document is to help SAP Security Administrators in understanding the SAP Security system audit requirement. This document is not intended for SAP Financial Audit and can only serve as guideline in preparing and planning for the SAP System Audit.

Audience

SAP Security User and Role Administrators and any Audit facing Compliance or Security Manager.

Guidelines

In the following sub-sections we will look at the general activities, processes and security objects and elements that Auditors look for, search for and ask for. As a general observation, a polite demeanor towards the Auditors instead of aggressive or defensive one will always help in cordial relationship between you and the Auditor. This ensures constructive approach towards the same goal of keeping your SAP System clean and secure.

These guidelines are based on the security guides of SAP which you can find at http://service.sap.com/securityguide.

In addition you may want to have a look at the Run SAP and E2E Solution Standards from https://service.sap.com/RunSAP. (See transaction RMMAIN in the Solution Manager, too.)

E2E Solution OperationsSAP Standard for Security
https://service.sap.com/~sapdownload/011000358700000666462009E/STD_Security_V10.pdf

Implementation Methodology: Security Design
https://service.sap.com/~sapidb/011000358700000685892009T/Accelerators/46DA314A27B3B758E10000000A4218A8/IM_SECURITY_DESIGN.PDF

Implementation Methodology: Security Setup
https://service.sap.com/~sapidb/011000358700000685892009T/Accelerators/C1DA314A27B3B758E10000000A4218A8/IM_SECURITY_SETUP.PDF

Implementation Methodology: Security Operations
https://service.sap.com/~sapidb/011000358700000685892009T/Accelerators/01DB314A27B3B758E10000000A4218A8/IM_SECURITY_OPERATIONS.PDF SAP Standard User ids

Report RSUSR003 (or transaction RSUSR003) can be used to run a report on SAP Standard user ids.

See Online Help:

Protecting Standard Users
http://help.sap.com/saphelp_nw70/helpdata/EN/3e/cdaccbedc411d3a6510000e835363f/frameset.htm

The Early Watch Alert report shows the status of the standard users, too. See https://service.sap.com/ewa for details about the Early Watch Alert.

The following table below describes the state of the SAP Standard User ids that can be considered fairly secure and has been adequate and satisfactory to the Auditors per the Audits that I have seen so far.

Standard SAP User id	Client	Default Password	Acceptable State
SAP*	000, 001, 066 or any Business client in any Production, Quality or Development system	06071992 Or PASS	User id SAP* Exist and is locked, and password is not trivial or default
DDIC	000, 001, 066 or any Business client in any Production, Quality or Development system	19920706	User id DDIC Exist and password is not Trivial. User id can stay unlocked but a policy to change its password on a regular interval.
EARLYWATCH	066	SUPPORT	Exist, Password not trivial and locked by administrator
SAPCPIC	000, 001, 066 or any Business client	ADMIN	Exist, Password not trivial and locked by administrator

1. There should be a policy to change DDIC password or any Dialog user id's password after a regular interval of time. You can set password expiration time through a profile parameter that will be discussed below in item 4.2. The policy should be stated in the Standard Operating Procedure and work instruction document for SAP Security.
2. Security Administrator should at least quarterly check Report RSUSR003 for the status of SAP Standard user ids and remediate incase of any discrepancies.
3. The following Authorization will be needed by Security Administrator to execute this RSUSR003 report.
    - Authorization object S_USER_ADM with the value CHKSTDPWD for the field S_ADM_AREA. If the administrator does not own this authorization the following authorizations are checked instead which require strong change authorizations (see notes 717123 and 704307 for details):
    - S_TABU_DIS – Activity – 02 and Authorization Group – SS
    - S_TABU_CLI – X Client Maintenance Allowed
    - S_USER_GRP – Activity – 02 and User Group – SUPER

Checking Profile Parameters

For any operating company Business and Audit requirement determines the values of the profile parameters. Below are the list and brief description of the various profile parameters that impact SAP Security and Audit and the best practices value that they might have to satisfy security and Audit requirement.

Profile parameter	Description	Expected Value
login/min_password_lng	Minimum length of password that user need to Input	8
login/min_password_digits	Minimum number of digits that password should contain	1
login/min_password_letters	Minimum number of letters that password should contain	1
login/min_password_specials	Minimum number of special character that password should contain	1
login/min_password_diff	Min. number of chars which differ between old and new password	>0
login/password_expiration_time	Number of days after which password expires and should be changed	90
login/password_history_size Available as of SAP NetWeaver 700	Number of old passwords that the system stores so that user cannot repeat old passwords	5
login/password_max_idle_productive Available as of SAP NetWeaver 700	Number of days till which password used by user remain valid and after which that same password cannot be used for login	60
login/password_max_idle_initial Available as of SAP NetWeaver 700	Maximum number of days for which initial password remains valid	7
login/disable_multi_gui_login	Disable multiple SAP logons for same user id	1
login/fails_to_session_end	Number of invalid login attempts until session end	3
login/fails_to_user_lock	Number of invalid login attempts until user lock	5
login/no_automatic_user_sapstar	Control automatic login using SAP* with default password in the case when user master record of SAP* has been deleted	1
rdisp/gui_auto_logout	Maximum time in seconds after which GUI session will automatically logout	3600
auth/object_disabling_active	Prevents disabling of Authorization objects by transaction AUTH_SWITCH_OBJECTS	N
rec/client	Activate or Deactivate Table logging in a client	ALL – which means table logging activated in All clients

Audit and Table Logs

Logs can be used in troubleshooting any issue or identifying any threat to the SAP system. Critical tables should be logged to see nobody does changes to these tables.

1. **Security Audit Log**: Auditors like to see a configured Security Audit log as it helps the security administrator in monitoring the SAP system. Security Audit log can be configured using SM19, can be displayed using SM20 and can be deleted using SM18. There are certain parameters that have to be enabled for configuring Security Audit log.

- rsau/enable – Should have value 1
- rsau/max_diskspace/per_day or rsau/max_diskspace/per_file : Either one should be set
- rsau/Selection_slots: Should be set to the value equal to the number of Filters needed.

Filters should be appropriately configured and is dependent on the level of Security you need and the amount of log that your system may store. This is how I will configure it:

Filter 1: Will have Client as * and User as * and for Event Class I will have all the Critical event class.

Filter 2: I use filter 2 to log details about successful and not successful RFC function calls to get information how to set up authorizations concerning theauthorization object S_RFC. This filter is only active as required.

Filter 3-n: Also I will have transaction and report started by critical users, like SAP* or the support users as I like to see the transactions or reports executed by these users.

It is important to note that if your Security team has access to SM19 and SM20, you should refrain from giving them SM18. SM18 should only be with Basis team.

SM20 gives very useful information like from what terminal, what kind of transaction or report was executed, using what user id, and at what time. A detail about configuring the Security Audit log is available on SAP help portal at http://help.sap.com/saphelp_nw70/helpdata/EN/c7/69bcb7f36611d3a6510000e835363f/frameset.htm.

There exists an additional ST01 trace viewer ZSHOWAUTHTRACE on SDN which you might find to be quite useful. See http://weblogs.sdn.sap.com/pub/wlg/16729 for details.

2. **Table Logging for Critical tables**: This is another item that Auditors scrutinize carefully as there are certain tables that should be logged for changes in Production or should be set as Non Modifiable.

- Please make sure Rec/Client is set to “ALL” to ensure table logging is activated in all the clients as previously discussed in item 4.2.
- Please check in transaction SE13 that Log Data Changes box is checked or in table DD09L for Field name LOG value should be X for the following tables as best practice. (You can use report RDDTDDAT_BCE or RDDPRCHK, too.)

T000	Clients
T001	Company Codes
TACTZ	Valid activities for each authorization object
TNRO	Definition of number range objects
TOBJ	Authorization Objects Definition
TSTC	Transaction Code Definition
TSTCA	Values for transaction code authorizations
OBJH	Object Headers Used

TSTCP	Parameters for transactions
TBRG	Authorization Groups
TDDAT	Maintenance area for tables
T009	Fiscal Year Variant
T042	Payment Transactions

This list can in no way be considered complete but something that has been seen in the projects that I have worked on.

- Below is the list of tables that the Auditors might check for Modifiable or Non Modifiable settings. It can be checked via t-code SE11 -> Tab Delivery and Maintenance -> Field Data Browser/Table view Maintenance or in table DD02L -> Field name Table Maintenance. (You can use report RDDTDDAT_BCE or RDDPRCHK, too.)

T000 (Clients)	Display/Maintenance Allowed
T001 (Company Codes)	Display/Maintenance Allowed
T009 (Fiscal year variants)	Display/Maintenance Not Allowed
TBRG (Authorization Groups)	Display/Maintenance Not Allowed
TDDAT (Maintenance area for tables)	Display/Maintenance Not Allowed
TNRO (Definition of number range objects)	Display/Maintenance Allowed with Restrictions
TOBJ (Objects)	Display/Maintenance Allowed with Restrictions
TSTC (SAP Transaction codes)	Display/Maintenance Allowed with Restrictions
TSTCA (Values for transaction code auth)	Display/Maintenance Allowed with Restrictions

System and Client Settings

The Following System Change Option should be set for Production environment. You or your Basis Administrator can check or set it using SE06 ->System Change Option or by using transaction SCTS_RSWBO004

1. Global Settings: Not Modifiable
2. Software Component: Not Modifiable
3. Namespace / Name Range: Not Modifiable

The following client setting should be set in Production

1. Client Role: Production
2. Changes and Transports for Client-Specific objects: No changes allowed
3. Cross-Client Object Changes: No changes to Repository and cross-client customizing objects
4. Client Copier and comparison table: No Overwriting
5. Catt and eCatt Restrictions: Catt and eCatt not Allowed

Maintaining User Groups

It is a good practice to have User groups maintained for the user ids in your SAP system. You can create User groups using t-code SUGR. It helps you as well as the Auditors when you have clear demarcation among all the IT users and the Business users. For example in one of my project, we had the following user groups:

1. IT Basis Admin
2. IT Security Admin
3. IT Batch Admin
4. IT Production Support – MM, SD, FI etc.
5. Business users – Regional
6. Business users – Operating Company X, Y, Z etc.
7. Terminated user group
8. Inactive user group
9. System user group – For System user ids
10. Super User group – For Super users like SAP*, DDIC etc

Also it will help if you have the same user group configured in Quality system. Auditors like to see your Quality system matches your Production system as much as possible.

Access to maintain user group Super should be tried to be restricted using Authorization object S_USER_GRP. For example if you have four Security Administrator in your team and not all need to maintain Super user ids then restrict it from them.

User Creation, Modification and Deactivation Process

1. Creating or modifying a user id in SAP Production system should only be done by the Security Administrator on the basis of some kind of Approval. Different Operating companies follow different processes like some may use hard copies of the SAP User Access form, some may use electronic version of it or some may just have approval via email. Whatever is the case, these user access documents should be retained for the Audit purpose.

   Note: Auditors might take a sample of user ids created in a period of time and then look for the user access approval document.

2. Similarly any deactivation, disabling or deletion of the user ids should have a procedure and should be part of SAP Security Administrator SOP. It could use the same format as is being used for creation or modification of the user ids.

   Note: Auditors might like to see that every terminated user is properly disabled from the SAP system. They might take a sample of users terminated in a period of time and ask for the user deactivation or termination document.

   Please make sure you get the information from your HR team for every user leaving your company and disable or deactivate them on a daily basis.

   Also if you do not delete the user ids in case of termination but disable those by changing the valid to date and lock them then please make sure that you have a method to differentiate users locked because of termination and those you have locked because of 90 days inactivity. One method could be to use a User group Terminated for terminated users and Inactive for users who are inactive because of not logging in the system for 90 days.

Process for Super User ids and System ids

There should be proper documentation on the process of how a Super user id (DDIC, SAP* or Custom Super user ids created with excessive access and critical transaction) is given to the user. The following guidelines can help:

1. Whoever requires this kind of access should specify the exact reason why this is needed. He should also specify the dates for which he needs it.
2. This kind of access should be approved through the approval process in place.
3. Open the Super user id for those many days and send the email with the user id and another email with the initial password.
4. Make sure Security Audit log is enabled for these user ids.
5. Once the user is done, **lock** the super user id again and take approval for the functionality that user has completed using this user id. Security Audit log can help you with this.
6. Make sure you are preserving the documents related to activation of the Super user id and the subsequent documents of Audit log and its approval.

Note: Auditors might take a sample of the number of times your Super user ids were activated and ask for the various documents on them.

Tip: Do not use SAP* as your Super user id. Remove SAP_ALL and SAP_NEW Authorization profiles from it and lock it. Create your own Super user id and activate it on the need and approval and then lock it again after the job is completed.

Auditors also might like to see how passwords are maintained for System user ids and how they are kept Secured. Make sure there is process around the System user ids as well.

Critical Transactions and Authorization objects

There are certain critical transactions that you should be careful about when giving in Production. Certain t-codes should only be given to the Security team, certain others only to the Basis team and few that should be restricted to be assigned only on the Super role that is only given through your Super user id.

1. **Critical transactions**: I will try to give the list of critical t-codes and the role where it should have in Production or even Quality. This list can only be considered as starting point to look in your SAP system and can vary depending on the business requirement of your company

Critical T-code	Role
SU01	Security only
SU01D	This is the display-only variant of transaction SU01 which can be added to other roles, too.
SU10 or SU12	Security only
PFCG	Only Display in Security only (restrict object S_USER_AGR, allow activity 03 only)
EWZ5 or EWZ6	Security only
SUGR, PFUD and SUIM	Security only
SUPC	Security only
ST01	Security or Basis
SM19 or SM20	Security or Basis only
SU02 or SU03	Security only (now obsolete)
SU20 – SU26	Nobody should really need in Prod. Lock in Production
SM18	Basis only
RZ10 – RZ11	Basis only

SA01	Basis only. Lock in Production
SAINT	Basis only
SCC4 – SCC9	Basis only. Lock in Production
SCCL	Basis only. Lock in Production
SE01 or SE03 or SE06	Basis only. Lock in Production
SE09 or SE10 or SCC1	Nobody should need in Production. Lock in Production
SE09 – SE13	Nobody should need in Production. Lock in Production
SM01	Security only
SM12, SM13 and SM14	Basis only
SM36	Basis or Background Admin
SM49 and SM69	Basis only. Lock in Production
SM59	Basis only (Use the new authorization object S_RFC_ADM if you have to grant display authorizations. See http://help.sap.com/saphelp_nw70/helpdata/en/84/d3eb4190966024e10000000a1550b0/frameset.htm for details.
SP01	Spool Admin and Basis
SPAD, SPAM and SPAU	Basis only
STMS and STMS_	Basis only. Lock in Production.

*	
DB*	Basis only.
SNOTE	Basis only. Lock in Production.
SA38, SC38, SA39 or SE38	Super User role (never use SE38 if SA38 is sufficient.)
SM30, SM31 or SE16	Super user role
MASS	Super user role
SECATT	Super user role
SE93	Nobody should need in Production. Lock in Production
SHD0	Nobody should need in Production. Lock in Production
SARA	Archive Administrator

2. **Critical Authorization objects**: As a general thumb rule, be aware of all Authorization objects that start with S_ like S_TABU_DIS, S_DEVELOP etc. Whenever you have to maintain them make sure that you read the documentation on them and understand them before maintaining it. Be careful with wildcarding * any field. Below we will look at few critical ones that should be added to roles with wise discretion.

   - S_ADMI_FCD: Normally needed only by Basis Administrator.

   - S_APPL_LOG: Nobody should have delete access to Application logs.

   - S_ARCHIVE: Create and Change activity should be in your Archive Admin role only and given on your Super user id with proper approvals.

   - S_BDC_MONI: Normally needed by Basis Team but can be needed by functional team if they are using LSMW to upload legacy data.

   - S_BTCH_ADM: Only needed by Basis or Background admin with value Y.

   - S_BTCH_JOB: Depending on the policy if you want your end user to have access to release their jobs, you can give this access with RELE. If they should have only access to schedule it then this authorization object is not needed.

   - S_BTCH_NAM: Only needed if you want a user to have access to run something in a background using a user id for which user himself does not have access.

- S_CALENDAR: Maintain activity should not be needed anywhere except in your super user role.
- S_CLNT_IMP: Needed by only Basis.
- S_CTS_ADMI: Needed only by Basis.
- S_C_FUNCT: Should not be needed by anybody except probably Basis.
- S_DATASET: Maintained with caution. Should not be wild carded for both ABAP Program and File path.
- S_DEVELOP: Again should be maintained with caution. Beware of DEBUG, PROG, FUGR object types.
- S_LOG_COM: Should only be in Background or Basis Admin roles.
- S_PROGRAM: It is a good practice to have your program or report check for S_PROGRAM. If it does good to have this object maintained accordingly.
- S_PROJECT: Should not be really needed in any role in Production.
- S_QUERY: Important to maintain or deactivate depending on if user need full access to just execute access to SQ01.
- S_RFC and S_RFCACL: Needed on the roles given to System id and wherever there is check for RFC.
- S_ICF can be used to grant authorization about who is allowed to use which RFC destination . You assign authorizations for this authorization object in the calling system of an RFC connection.
- S_RZL_ADM: Should not be really needed by anyone except Basis.
- S_SPO_ACT and S_SPO_DEV: Should be maintained carefully. Normally only Spool Admin or Basis Admin should need them. End users can have SP02 for which they do not need these objects.
- S_TABU_DIS: Should always be maintained with caution. Activity 02 (Change) should be controlled with Authorization group.
- S_TABU_CLI: Should not be needed by anybody except Basis.
- S_TCODE: Should be always checked for range or wildcard * on the TCD field.
- S_TRANSPRT: Not needed in any role except Basis in Production.
- S_USER_*: Should not be needed in any role except Security. Use the display activities 03 and 08 if required.)

Change Control Process

Auditors like to see the process involved around the movement of Transport Requests from Development to Quality and then to Production. The following points should be kept in mind:

1. Typically there should be some kind of Scope Change Request or a Production Problem report that initiates the Change.
2. The change request should be approved by the Change Control Board before being worked on in the Development system.
3. Once the change has been unit tested in the development environment and the transport is created for it, it should be formally approved again for its transport to Quality system.
4. There should be some kind of Formal script that is executed in Quality system to test the new change. It is advisable that this script should also do regression testing to check the impact of this new change on the existing system.
5. The Change Control Board should review the already passed formal script before approving its transport to Production. Ideally there should be some fixed time and day when changes should be transported to Production instead of moving it anytime. This help in being ready for any adverse impact of the new change to the existing system.

Common Audit Observations which should not occur in productive systems

1. End users or Business users have DEBUG access in Production. Sometimes even the DEBUG-replace activity 01 is assigned.
2. Security has access to delete Security Audit log files.
3. Users other than Basis have access to modify Cross Client tables.
4. Users other than Basis have access to schedule and release any jobs under any user id.
5. Using &SAP_EDIT functionality users can update tables even with SE16N (SAP has removed this function with note 1420281.)
6. SAP Standard user ids are not maintained properly.
7. Profile parameters are not set properly.
8. Security Audit log is not implemented.
9. Critical tables are not logged.
10. No formal process for User Maintenance.
11. No formal process for assigning Super user ids.
12. IT users having Business functionality and vice versa.
13. System and Client settings are not secure.
14. Termination process not properly followed.
15. No Formal Change Control process.
16. The authorization profile SAP_ALL is used. (see http://help.sap.com/saphelp_nw70/helpdata/en/78/7a553efd234644e10000000a114084/frameset.htm for details.)
17. The authorization profile SAP_NEW is not resolved and deleted. (see http://help.sap.com/saphelp_nw70/helpdata/de/8a/7b553efd234644e10000000a114084/frameset.htm for details.)

Related Content

http://service.sap.com/securityguide

http://service.sap.com/security

http://www.sdn.sap.com/irj/sdn/security

http://help.sap.com/

Disclaimer and Liability Notice

This document may discuss sample coding or other information that does not include SAP official interfaces and therefore is not supported by SAP. Changes made based on this information are not supported and can be overwritten during an upgrade.

SAP will not be held liable for any damages caused by using or misusing the information, code or methods suggested in this document, and anyone using these methods does so at his/her own risk.

SAP offers no guarantees and assumes no responsibility or liability of any type with respect to the content of this technical article or code sample, including any liability resulting from incompatibility between the content within this document and the materials and services offered by SAP. You agree that you will not hold, or seek to hold, SAP responsible or liable with respect to the content of this document.