Appropriate SAP workstations for internal auditing

Roger Odenthal

1 Introduction

Audit review with SAP processes has been dealt with many times in well-founded audit literature. Regardless of this, many commercially-oriented audit colleagues still fail, even before they can conduct that first audit that they have planned with so much enthusiasm, at the point of setting up an appropriate SAP workstation. Such failures are regrettable in light of the operational philosophy of SAP software as a “supportive resource” in handing primary operational processes. Its control and audit cannot rest primarily on the work of a few technically determined IT auditors. Rather, effective risk management in the SAP environment requires not only their indispensable expertise, but also the watchful supervision of functionally responsible employees and appropriately targeted auditors. This publication is for them. It is intended to assist them in surmounting both actual and perceived obstacles, in order to set the foundations for an effective audit.

2 It begins with the operating environment

In order for SAP data to be audited, it is viewed on a computer screen, saved locally, transferred via interfaces, prepared with auditing software (ACL / IDEA) and printed out in working papers. The operating environment to be set up should take these general requirements into account.

Practical considerations in this case would call for local computer workstations, which would enable a sufficiently rapid and reliable communication with the SAP process. These should be equipped with the usual Office package, in order to enable the standardized data exchange between SAP and the excel calculation software, for example, or the preparation of working papers. The same applies for audit software, if it is part of the standard internal audit tools. In addition, two-step audit processes require the setup of a data directory with unrestricted read- and write rights, in which SAP data could be stored if needed. In the analysis of large amounts of data using audit software, an internal hard drive is preferred over a network drive, for reasons of speed.

3 What rights?

Less fruitful discussions on the appropriate SAP rights can be avoided by the use of standard role templates. For many years, SAP has made appropriate authorization role templates available in its systems for the various tasks of internal audits. With only a few exceptions, these include only read functionality, and can be adapted to operating requirements at a reasonable cost. The following steps are necessary for this:

- Identify roles and transfer them to the customer name area

  Prepared role templates include the designation “*AUDIT*” as single and group roles, and can be determined in this way.

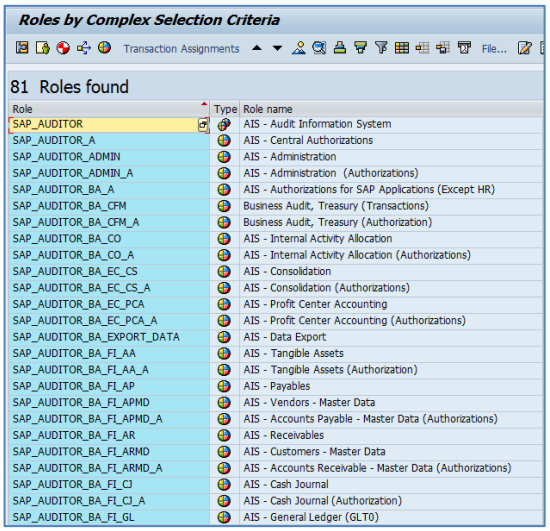

Figure 1: Standard SAP role templates for auditor purposes (example)

There are two versions of each individual role, as shown in the example below

– SAP_AUDITOR_BA_MM_PUR **(Menu** Commercial Audit, Purchasing**)**

  These roles, without the "_A" at the end, contain *no rights.* The auditor has only the SAP menu surface necessary and adjusted for his/her activity (user menu) with the designation (AIS - Audit Information System).

– SAP_AUDITOR_BA_MM_PUR_A **(Rights** Commercial Audit, Purchasing**)**

  These complementary authorization roles with the suffix "_A" already include all activity rights adapted for the menu roles (read functions only). However, they need to be supplemented with regard to company organizational elements (information on permitted company codes, etc.).

As a rule, it makes sense to assign the auditor both complementary roles for all audit fields. If discussions occur concerning the read rights in individual instances, it is recommended that the first step be to assign the menu roles that are not affected (without authorizations). As a result, the audit will receive a modest SAP work area (AIS audit surface). In this case, concrete access rights to the listed menu areas continue to arise from the individually and operationally created authorization roles for the audit.

- Add organizational authorizations (only in authorization roles)

  Within the role templates (exclusively authorization roles), necessary organizational authorizations can be added after transfer to the customer name space.

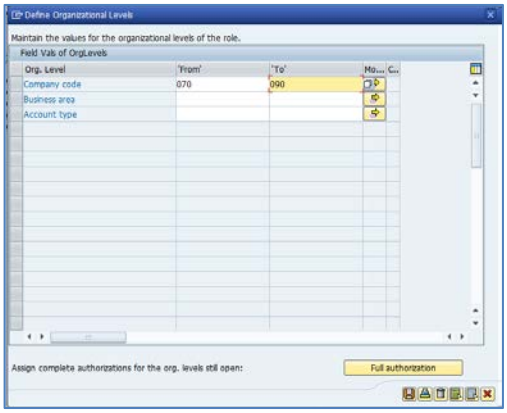

Figure 2: Adding organizational authorizations

These are to be coordinated with the audit. As a rule, full authorizations (e.g. "*" for all accounting areas) are entered for internal audit tasks.

- Account for exceptions

  Differing from the course of action outlines above, a few audit roles, listed below, require special assessment, since they, as exceptions, have "change authorizations:[1]"

Role template	Content	Recommendation
SAP_AUDITOR_ADMIN_A	Includes table maintenance	Do not assign
SAP_CA_AUDITOR_SYSTEM	Various maintenance activities	Do not assign
SAP_AUDITOR_TAX_HR	Table maintenance	Change activity for object S_TABU_DIS to value "03"
SAP_AUDITOR_BA_A	Manage DART exports	Remove activity level "02" from the objects F_TXW_XX
SAP_AUDITOR_TAX_DART_A		

The properly selected and adapted authorization roles can be finally grouped into an "Internal Audit" composite role, and transferred to the auditors.

4 A few specialties!

The authorization rights setup and assignment as shown above reflects the usual process. This should be fairly easy to implement and has the additional appeal of allowing the auditors to use the AIS auditor user interface (as an individual SAP user menu). For optimum SAP working conditions, the following *additional fine adjustments* are recommended:

- Supplementary authorizations for transaction calls (for object S_TCODE)

  Transactions (SAP functions) and their related activity options (e.g. view, change) must be considered *separately* in the SAP software! For example, the activity level can be limited to viewing functionality, even for access through a "modifying" or "maintenance' transaction. This is useful for the audit, since a great deal of audit-relevant information can be determined only from such transactions.

  Since the audit roles shown are generally limited to read-only activities, SAP transactions can be assigned more generously to them, without presenting a hazard for data or from operator errors. Typical examples are:

  – SE16 Table maintenance (viewing functionality only)
  – S_ALR* Calling up various ABAP list reports
  – OB* Maintenance dialog for customizing tables

  As well as access for many other basic functionalities (viewing LOG protocols, update programs etc.) that cannot be listed separately here.

  There may be objections due to the access to sensitive information (CO, HCM) or the inadequate upgrade capability of such roles (transaction SU25). In these cases, a useful practice has been to provide a practical test phase with the transactions already included in the roles, to be expanded as needed.

- Download authorization for SAP data from reports and tables (for object S_GUI)

  The analysis of SAP data using special audit programs on locally operated computers requires download authorization for the auditor. (Activity Export – 61)

[1] See Tiede, Thomas: *SAP* R/3 Ordnungsmäßigkeit und Prüfung des *SAP*-Systems

- Download and upload authorizations for favorites

  Procedure models for certain audits in the SAP environment are frequently developed based on menu favorites and exchanged between auditors as prepared audit interfaces. In order for these to work and so that existing favorites can be assigned to the appropriate SAP audit users as required, download and upload authorization for favorites is required.

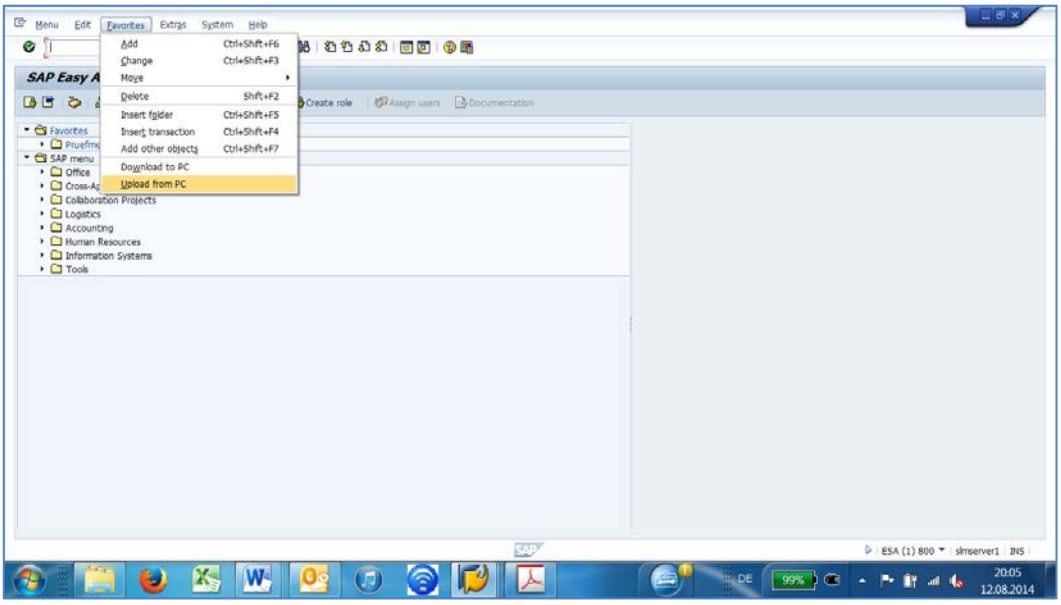

Figure 3: Need-driven loading of favorites by auditor

- Manage their own user profile (fixed values and parameters using transaction SU3)

  For assigning and setting up printers, as well as pre-setting download paths and other organizational tasks or selection criteria, the auditor's own user profile (fixed values and parameters) should be manageable by the auditor.

- Using variant technology, background processing and job control

  SAP analyses of complex audit questions must not affect the dialog processes of other SAP users. With the appropriate authorizations, it is preferable to save these within the SAP system using variants, for repeated use by the auditor. Subsequently, they can be planned and released in the background (at off-peak periods or continuously, e.g. as annual analyses).

- Changes to variables in the tables "TVARV / TVARVC" (for object S_TABU_NAM)

  In order to set up dynamic report variants for repetitive or variable audits, SAP provides the tables listed. Apart from the limitation to viewing authorization, auditors should be able to enter audit-related variables into these tables and assign selection values. In order to limit a change authorization exclusively to these special tables, SAP provides a new authorization object "S_TABU_NAM." It should be activated and change authorization given to the auditor. Details can be found in OSS note 1481950.

- Assignment of the SAP audit users to query user groups

  SAP provides some premade audit programs (queries) on a standard basis for the audit. These support both document analysis and data transfer to ACL / IDEA audit software using special interfaces. In order to use these, it is necessary to assign die audit IDs to the following query user groups:

  – /SAPQUERY/AU Audit

  – /SAPQUERY/AM Attachment manager

  This also applies if the SAP audit user does not have the authority to set up or change queries!

5 *The auditor does the designing here*

After being granted the authorities outlined above, the auditor now has some design options within the SAP system, which he/she can now use independently:

- Setting up the printer for sufficient working papers

  First it is sensible to select an appropriate SAP standard printer or local printer with connection to the auditor's PC; this is done in the user preferences (transaction SU3) using the tab "Default" and the heading "Spool control – OutputDevice." For traceable working papers, before the first print job use the "Properties" button, change to the "Cover sheet" option, and permanently activate the "Selection cover sheet."

- Presetting the area menu

  The use of specific user surfaces with the user menu (e.g. AIS) and favorites has already been mentioned above. This represents another service option. Within the SAP standard menu, separate large or small menu trees can be identified as so-called "area menus." To do this, the menu node is marked. The button [Options | Detailed technical information] leads to the corresponding menu names.

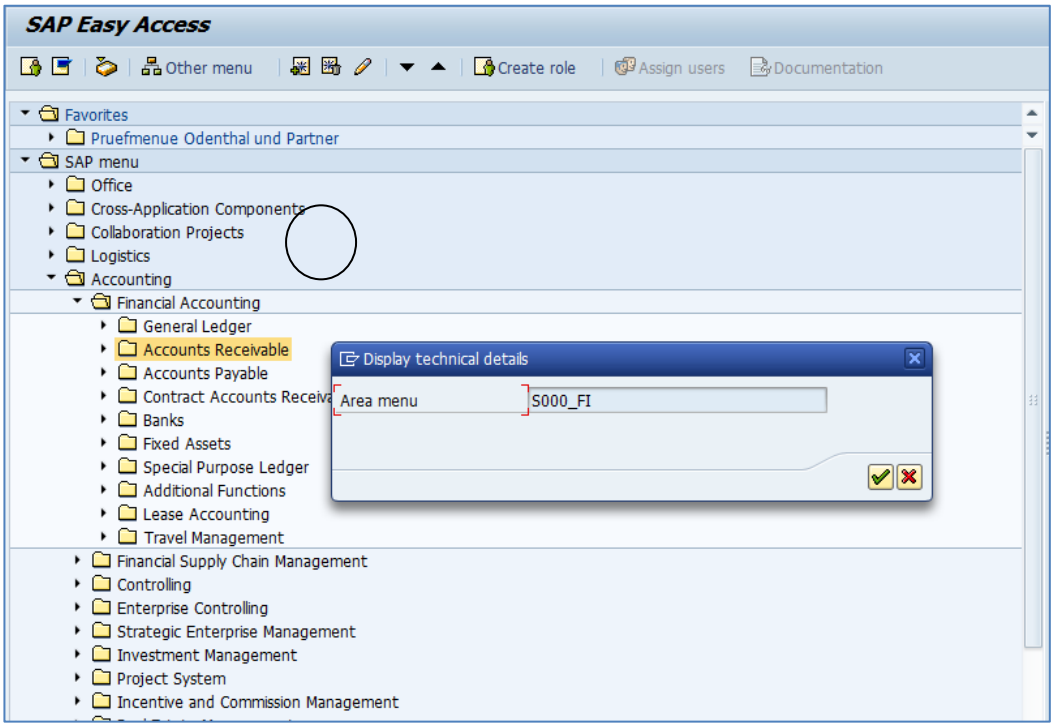

Figure 4: Identifying an area menu

Using user preferences (Transaction SU3) and the "Default" tab, this entry can be used as the "Start menu" (user interface) for a special audit.

- Setting up user parameters

  Previously overlooked by most people, personal user parameters can substantially increase the feel-good factor when using the SAP process. They are available to the auditor also as part of user preferences (Transaction SU3) by clicking on the "Parameters" tab. So, for example, selection criteria for data evaluations can be automatically managed, access options for queries expanded of download paths for audit results can be set; below are a few examples:

  – GR8 (set download path / directory)
  – GR9 (set upload path / directory)
  – AQW (query work area with entry of "G" for AIS evaluations)
  – AQB (query user group with entry of "AU" for Audit)

- BUK (company code)
- BAR (document type)
- GJR (business year)
- BIL (balance)
- KPL (chart of accounts)
- GLN (ledger)

A complete overview of the available parameters and their meaning can be found in the tables “TPARA” and “TPARAT.”

- Setting up the SAP interface

  One last look will lead to the local appearance of the SAP screen. If SAP access is done using the SAP-GUI components, then its configuration button can be used to open up numerous setting options for design, color, font types and sizes, as well as codes, all of which can simplify SAP operation.

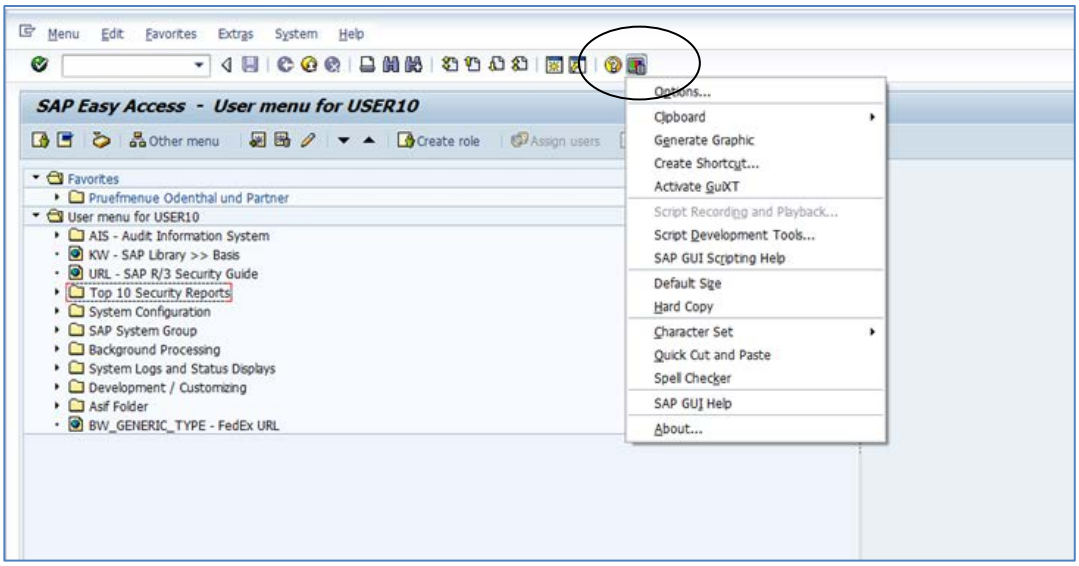

Figure 5: Individual setup options for the SAP interface

6 Summary

Setting up an appropriate SAP workstation for commercially oriented auditors presents challenges for all concerned in its design within the SAP process. One clear technical point of orientation is the audit order, which generally is sufficient to describe the access areas and rights. It can be transferred to the digital environment with the same effect, which should largely eliminate the need for discussion on content authorizations between the operational audit area and the SAP administration. Independent of this, in individual cases some *technically* justifiable access limitations may be sensible, and which the audit in return can understandingly allow. Building on these basic positions, satisfactory solutions can frequently be reached in a recurring setup process.