

Figure 1

How to audit SAP -WORKING PAPER-

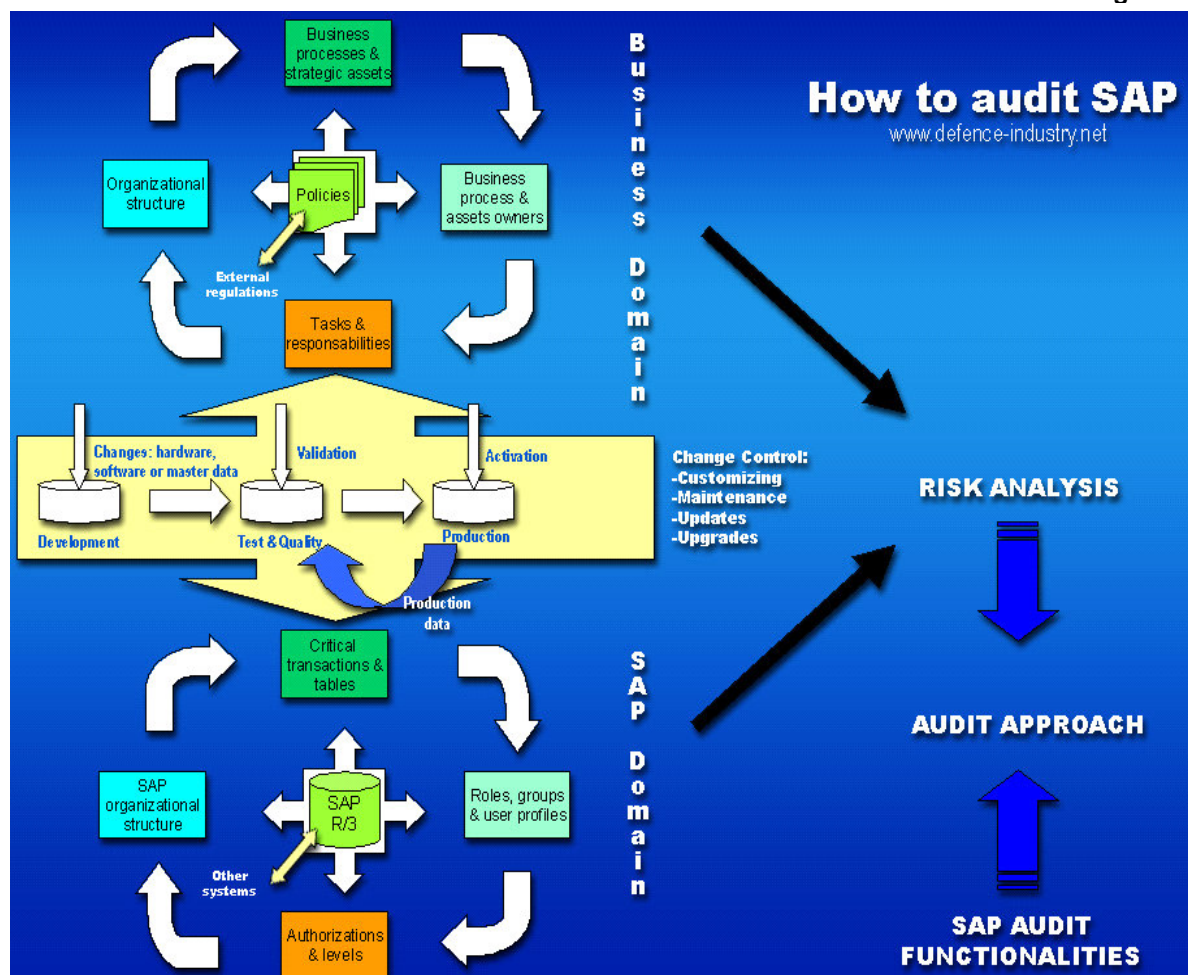
Please do not quote

K.C. Davids
J. Durant
W. Mouthaan¹

Introduction

Did you learn a lot about SAP, customising, implementation and keeping it running within your organisation? Are you conscious about the many risks and therefore still wondering where to start with you're auditing activities? In this article we will give you a practical guide line to set up and start a cost-effective audit program.

The guide line consists of four parts. In part one we explain the concepts of the business and SAP domain and their relationship. Understanding this concept will help the auditor to identify critical risks to focus on. In part two we introduce the elements for setting up an audit program.



Understanding these elements may help the audit organisation to define their requirements to set up an effective audit program for their specific situation. Part three of this article gives the reader a recommendation how to start audit activities effectively. In part four a real live

example is described. The article ends with a summary.

This article is written for audit managers and auditors with basic knowledge of SAP and who are interested in how to use SAP for their business audit programs.

¹ K.C. (Christiaan) Davids MSc is a teacher and researcher at the Netherlands Defence Academy.
J. (Jerry) E. Durant MSc and is certified as a CST, CQA, CISA, CSP and CICS, and serves as Managing Director of Certellus LLC.
W. (Wouter) Mouthaan MSc is IT-auditor at the Ministry of Defence of the Netherlands.

PART 1: BUSINESS & SAP DOMAIN

Since a picture can tell us more than thousands words, we will explain to you the overview as depicted in the figure 1. Understanding the relationships as shown in this conceptual model improves decision making to set up and execute your SAP audit program.

Alignment within the Business Domain

To introduce SAP in your organisation successfully one has to establish a clear understanding of the business which will be supported by SAP. We will call this the Business Domain. In the Business Domain the policies of the organisation must be consistent regarding goals, objectives, defined organisational structure, business processes and the company's strategic assets. Business process owners and the owner's strategic assets should be defined. It is necessary that tasks and responsibilities are defined which are derived from a process of rethinking the business. In practice no single organisation has all above clearly defined since organisations are changing continuously due to the need of adapting its operations in ever increasing dynamic environments.

Tip for the auditor:

The auditor can help management to identify risks due to inconsistencies within the Business Domain.

When there is not enough alignment within the business domain the implementation of SAP and integrity of information when running SAP will be at risk per definition.

Alignment within the SAP Domain

SAP is an application which uses transactions to change data in tables which are stored in a database. To make SAP work customisation has to be done in a consistent way. SAP requires a defined organisational structure. Within and through this structure one has to define transactions and related tables to be customised. Furthermore one has to define roles, which can be clustered into groups, and user profiles. User profiles may consist out of a selection of roles and these roles could also be combined in a group. At the end groups can be addressed to a user profile. The last important step is to define the right authorisations and authorisation levels.

Tip for the auditor:

The auditor can support management to identify the critical transactions and evaluate the defined roles and groups and user profiles based on the principles of separation of duties.

Furthermore the auditor can find inconsistencies in authorisations and authorisation levels.

Integrated Risk Analyses

The conceptual model makes clear that the business domain and the SAP domain are related to each other. To set up an effective audit program one should consider the risks integrated from both domains.

Different environments and transports

When changes appear in the Business Domain this will reflect in changes in de SAP Domain. To effective manage the change control different environments have to be defined and implemented. Therefore protocols changes are made in a separate development environment and than transported to a separate test & quality environment. After testing and quality control procedures the change is activated by transport to the production environment.

Tip for the auditor:

The different environments and transports should be part of the audit program since this area contains risks that could hazard the consistencies between de business domain and SAP domain.

PART 2: HOW TO SET UP YOUR INTEGRATED AUDIT PROGRAM

Audit approach

The application SAP provides auditors useful information to support auditing the integrity and security of information management by SAP itself. Different reports and the highly 'clickable' screen architecture of SAP can be used to find inconsistencies. Nevertheless auditors have to rely upon their own experience and knowledge or consulting expertise to find the issues with the highest risks for the organisation.

Figure 2

Lining up your fellow Auditors

How do you line up your audit organisation (i.e. a corporate audit organization) to dive in to the SAP jungle? More important; how do you communicate with the management of your organisation? What you need is a complete audit program, a concept to manage the SAP opportunity successfully. In this section an audit management concept will be developed. In the last section you can find a method were to start, in the business, SAP or in both domains at once.

As before we introduce an overview depicted in figure 2. Understanding the relationships as shown in this conceptual model helps the change management process in your audit organisation, the communication with management and decision making to set up and execute your SAP audit program. The concept consists of five major building blocks that cannot make a building by themselves. In other words this is an ongoing process where you need them all. The concept proves useful for managing the implementation of SAP as well as managing the live SAP system.

Risks Identification

The model starts with identification of risks. This part of the model can be used in many ways and with different instruments. Here you sit down think, brainstorm with your co-workers and last but not least communicate with the



managers of the business. It all comes down to what kind of SAP system you have. Is the system only for financials, or are the core business processes also covered? You can start this building block by making an analysis of the core SAP processes and then filling in what can go wrong. Be sure to write them all down; don't try to make a selection in priority yet.

*Tip for the auditor:
You can use the Business-IT alignment model from Maes. This model gives focus on the difference in strategic, tactical and technical risks.*

Managing Risk based Audit needs and objectives

In this step you start to cluster and breakdown, if necessary, the already identified risks in smaller pieces till you get neatly scoped main risks and sub risks. You are now set to prioritise the main risks with help from the sub risks. To do this the main risks should be split into a probability and damage factor. This step can, of course, be done with help from co-workers and managers, remember if they have something to say about this they are more motivated to support future audits. How you scale the chance and damage factor does not really matter, be sure though if you use figures to keep in mind that these kind of figures are no absolutes. This is just a tool to focus on what really matters.

Tip for the auditor:

A plot of the risks is an excellent tool for communicating with management. An integrated overview is an asset for them and gives the auditor the chance to discuss thoughts on a focussed way.

Audit plans and Projects

After communicating with business managers, audit managers and auditors and deciding what will be audited in the near future you can define audit needs on priority basis. Audit needs consist of an audit leader, goal, scope, capacity, time and target audience part. The needs are the starting point for audits. The needs can also be formulated as project plans or other forms you are comfortable with.

Tip for the auditor:

Risk and needs that are not utilised in the near future can be used some other time. A thorough view on the risk- and audit universe is very useful to signal and predict risks before they happen.

Portfolio Results for Management

Now you have audited in the business you may be tired and think well that was that. Be sure to wake up, your new knowledge can get to work. On the basis of what you have seen and the information on the risks you have been getting you can adjust the initial probability and damage. This is very important because the more audits you do the better the probability and damage (the risks) reflect the real world and can be used to inform management on what is really happening. It is also possible that you get new insights and spot new risk or other risks to be dealt with. This information is input for the first building block. Thus adjusted risk can go directly in the plot on the right side of the model to be communicated. New insights or other risks go to the initial step and have to be clustered. The circle is now spinning!

Tip for the auditor:

You can use all kinds of information to adjust the prioritisation of the risks. This is very useful in understanding the business and understanding the SAP environment.

Set up and maintain audit goals & strategy

The last building block is not part of the circle but is actually the *crowbar* to keep the wheel from spinning down. To get your audit organisation

up to speed with SAP and to inform them about your plans you need to write your idea's down, make decisions, pinpoint dedicated people and manage all the information that flows in your organisation once you get started. For this you can formulate an overall plan where you can clarify the different building blocks. If your organisation is not experienced with SAP it is necessary that you formulate, as part of the overall plan, a knowledge and training plan to invite your auditors in the SAP world and to keep the incoming knowledge in your organisation. Don't underestimate the change management that has to take place in your audit organisation before everybody really knows what SAP is all about. Even if you work at an organisation that is already comfortable with SAP it is useful to retain knowledge.

Tip for the auditor:

If your audit organisation is not ready for SAP yet and the tanker is coming real soon you can install a project team to get started. This project team should constitute of auditors from different branches of your organisation. Remember this is a process of change and you can reduce uncertainty if you invite them to be a part of the future.

PART 3: HOW TO START AUDITING YOUR BUSINESS EFFECTIVELY USING SAP

Prepare yourself

As stipulated in part one of this article the business domain relies upon the quality of how SAP is being defined, used and maintained. This is the reason why SAP BUSINESS audits should be executed to audit your business properly. The SAP BUSINESS audit isn't particularly unique from doing a regular audit, except that there is a new device (the SAP application) that must be contended with. Auditing of a business within a SAP environment, is an exercise in evaluating the configuration (BASIS) and implementation of the SAP application, therefore we call this the SAP BASIS audit. We are not auditing SAP; rather we are auditing how the product has been deployed. Because of the enormous complexity of the application it is essential that proper training be received, a work plan is set about, and that expert oversight is employed. These are essential, and without these fundamental elements the likelihood of success is marginal. How to manage these essentials is explained in section two.

With the introduction of the SAP Business and SAP basis audit type we refine the audit approach from section two further. Last, if you look at the picture in section one you also see the logic in separating these two audits types.

Understand SAP audit benefits

The use of SAP (or for that matter any ERP application) is a tremendous opportunity to take manual elements (roles, authorities, workflow, policies and practices) and embody them into an automated framework, thus creating a forced automated compliance. This term, "forced automated compliance", is scary for some and often gets equated with inflexibility. In fact, it provides a base for controlled flexibility, rather than simply looking at what it manages. Likewise, automated implementation (roles, authorities, workflow, policies and practices) of manual elements creates an opportunity for historical audit trails of changes, compliance variation management, and establishing an active repository for these items. This affords management a significantly greater level of comfort about control of the enterprise wide application environment. An item worth mentioning is that the process of manual to automated implementation of these elements has many positive benefits such as forcing us to revisit our control structure, examining role separation, more formal understanding and negotiation of cross organisational relationship, and whether change needs to be put into play (and by whom).

Start with auditing SAP BASIS

A couple of reasons why we start with auditing SAP BASIS is that the deployment structure/method has a profound effect on the entire environment and therefore the business. The BASIS audit also forces one to look at SAP administrative authorities and to question why a person is allowed to have a certain level of privilege. At least initially, these authorities are

necessary to simply configure and implement the system, thus reason by necessity. But once the application is live and operational, even at a basic fundamental level, the privileges need to be reduced and separated (segregation of duties) and defined in alignment with the business policies. Starting with SAP BASIS allows the auditor to acquire an additional level of understanding SAP and its implementation. This understanding can be used the scope the audit universe as explained in section two. The SAP BASIS audit is further a possibility for the auditor to acquire a rudimentary understanding from the configuration of SAP if, for whatever reason, the auditor has not been a part of the implementation of the SAP system.

Value on the education acquired through the BASIS audit.

Using current business function audit programs, i.e. financial, operational, legal, we can with the knowledge from SAP BASIS employ (use) SAP to carry out the SAP BUSINESS audit in an efficient and effective way.

Example: if an audit program calls for a review of outstanding purchase orders, the auditors would go into the procurement module and select a report that shows them a list of outstanding purchase orders. They could also use the Audit Information System (AIS - SECR) portion of SAP to conduct the same sort of extraction. Or, they could look to the table(s) involving purchase orders, closed purchase orders, and extract a set of purchase orders that are still open. Three methods, all having the same result, but each of which would be unknown unless they have training and hands on experience (thus the reason why BASIS examination first).

A by-product of the SAP Business Audit is knowledge about the SAP environment. With more information available about the required functionalities and performance of SAP to support the business we can do the 2nd round of doing the BASIS audit. A question which all auditors and audit management must ask is whether the SAP Audits (BASIS and Business Audits) should be done on a continuous basis or cyclical.

It is self-evident that as the application is utilised more and more that it will be examined, in a variety of different ways, on a continual basis. The only question that remains would be the frequency of the BASIS examination. One method of staying on top of this area is through the connection with the change management process. This will help audit management to stay informed about the quality of the

SAP configuration and the alignment with the business. In section two we explained how to manage all the information regarding audits and how to communicate this with the operational managers in the business.

REAL EXAMPLE: SAP BASIS AUDIT

Assignment

The audit project was requested by the Chief Financial Officer (business owner)

Audit needs

Audit Objective - SOX compliance with respect to separation of duties and transactional access risk remediation. The audit need out of the business domain requests for an SAP BASIS audit in the SAP Domain.

Audit object

Client had been a SAP installation site for about five years. A number of administrators had been involved, each having their own methods of implementing roles and profiles. BASIS Administrator was also the Database Administrator, and changes were allowed to be made directly into production and not via the appropriate method of Development to Test/QA then final transport into Production.

Audit Approach

The project involved a complete review of transaction level authority for approximately 175 users. Once a base of transactional remediation was established a method was employed to remove their authority without disturbing those who still were allowed role level access to those transactions. Since this was a time critical project the team did not have the opportunity to create new roles (rather copies

and removal was performed). The project took approximately 700 hours and involved 175 users and 49 base roles (involving critical transactions), with 1060 user/role combinations and 5403 transaction/role relationships.

Obviously there were a number of issues that effected the time required ranging from the period of neglect, extent of change, connection dependability, and even basis access. Of the 700 hours that 60 hours was efficiency losses as a result of these matters.

Outcome

Significant control risk reduction. In addition the impact of inconsistent SAP administration had resulted in various methods of role construction, and profile administration. The task was made more difficult because composite roles (a single role made up of multiple individual roles) and inconsistent generation of role profiles (some were not generated which created a gap when looking at transaction to role relationships). The later, role profile generation, while still allowing transaction level authorities created a material weakness in the audit trail of transaction to role relationship evidence. Despite these issues the outcome was positive and will allow the organization to establish a long term plan for support of the SAP environment and to make appropriate control improvements.

Conclusions

The example illustrate several things:

- a) ERP (enterprise resource planning) systems like SAP needs to be consistently maintained,
- b) The relationship of business process to system implementation is important, c) The process of doing an SAP BASIS examination provides an opportunity for global understanding of the business as well as the technology (some interesting things also get discovered outside of the scope of the examination), and d) SAP sustainment relies on understanding the status of the ERP (in this case the initial set up of authorities within SAP).

PART 4: SUMMARY

In part one we explained the characteristics of aligning the business domain with the SAP domain with adequate change control. These three major audit objects may be broken into smaller audit objects but it is important to recognise the overall picture for setting up an affective audit program.

In part two we described the elements to consider for setting up your effective audit program. We stressed that an audit program should be based on the five mayor elements of risk identification, identifying audit need and objectives,

managing audit plans & projects and communicate the results & evaluate new insights. All of these elements are aligned with the fifth and central element: your audit goals and strategy.

In part three a recommendation is given where to start your audit activities. We advice to start auditing the initial configuration of SAP (SAP BASIS), since the quality of the configuration of SAP defines the quality of your business transactions with SAP and therefore influences directly the quality of your business.

We hope that this article has started up or enforced your insights and approaches for your audit program.

Contact info

Please send us your feedback and mail us at:

info@defence-industry.net
www.defence-industry.net

CERTELLUSLLC@earthlink.net
<http://certellus.tripod.com>