How to Efficiently Conduct an IT Audit – in the Perspective of Research, Consulting and Teaching

Gabriel FELLEY
Institute for Information Systems, School of Business
University of Applied Sciences and Arts Northwestern Switzerland
CH-4600 Olten, Switzerland

and

Rolf DORNBERGER
Institute for Information Systems, School of Business
University of Applied Sciences and Arts Northwestern Switzerland
CH-4002 Basel, Switzerland

ABSTRACT

This article reflects the topic of IT audit – information technology audit – with respect to research, consulting and teaching. The expression 'IT audit' comprises information systems audits as well as information security audits combining the short-term to long-term management of the IT infrastructure with its daily operation in order to achieve the organization's objectives. No overall common standard procedure for an IT audit works generally.

However, standard procedures for IT audits, e.g. ISO 27001, are available, which must be particularly adapted and customized to fulfil a company's needs. This task requires experts. Thus, students of all Information Systems Bachelor or Master programs are trained to work in IT audit projects or even to lead them. This paper presents a case study, concerning the IT audit of organizations acting in the Swiss social insurance environment. The derived concepts are discussed. A best practice of knowledge transfers to students in the perspective of relating research and consulting is described.

Keywords
IT Audit, Information Security Audit, ISO 27001, Information Security Framework, Information Security Management System, Social Insurance

1. INTRODUCTION

The proposed article is about the interrelation between research, consulting and teaching of the cutting-edge topic most organizations are confronted with: IT audit. The IT audit, i.e. the information technology audit or information systems audit, has evolved from the management side of managing the IT infrastructure and the technical side of operating and cooperating in the right and latest ICT (information and communication technologies) in order to achieve an organization's objectives.

Depending on the vast amount of different types of organizations and their various internal setups, there was no easy common standard procedure to perform an IT audit. Thus, research that had already started in the last century, was mostly resulting in a kind of best practices, respectively guidelines. Nowadays, most of the organizations are forced or at least decided to do IT audits – normally within consulting projects or consultancy-like tasks. Standard procedures for IT audits, e.g. ISO 27001 [1], are available, but must be adapted and customized first [2] [3].

Furthermore, nowadays, students of all Information Systems Bachelor or Master programs are trained to work in or even to conduct IT audit projects. To train them well, professors need to have special skills: They have to combine and teach knowledge obtained from both research and consulting, in order to present their students with the entire picture of today's state of IT audits.

In the following case study, concerning the IT auditing of organizations acting in the Swiss social insurance environment, we present a best-practice of knowledge transfer to students in the perspective of relating research and consulting in order to generate the synergies from which both activities and particularly the students can benefit.

2. FINANCIAL IMPORTANCE

The Federal Social Insurance Office (FSIO) is the national center of expertise on policies related to old-age, invalidity and family. It plans, manages and monitors the corresponding social insurance systems to ensure that they function effectively. In addition, the FSIO initiates and coordinates reciprocal social security agreements with other countries. The Swiss Confederation spends about one third of its budget on social welfare. In recent years, this amounted to about CHF 20 billion for Switzerland, being a small country with only about 8.3 million inhabitants.

3. STRUCTURE OF THE SOCIAL INSURANCE NETWORK IN SWITZERLAND

The insurance network is structured along two main dimensions: The political or geographical dimension which reflects the 26 different cantons, the constituent states of the federal system of Switzerland. Each canton owns its own social insurance offices. In the other dimension the offices have organized themselves in different functional pools to ensure an optimal development, delivery and support of the IT services required to maintain a high quality execution of the numerous tasks of the related business activities.

4. SECURITY ISSUES

Together with the chief security officers of two main pools, the author has formulated an information security policy and developed a specific methodology to audit the corresponding offices. These two pools assemble more than 80 % of all the offices. The IT services which they deliver to the different offices, manage highly critical personal data and are responsible for a timely and correctly executed huge money transfer. Therefore, an appropriate information security policy applicable to all offices which want to preserve a large autonomy and a pragmatic way to conduct IT audits, is of essential importance to ensure the establishment and maintenance of a corresponding high security level.

The following article shows the main guidelines of the security policy and how it is linked to the ISO 27001 standard and other relevant country and branch specific regulations [4] [5]. The core element of the audit consists of a questionnaire, segmented in different categories: Feedback from the last audit (what improvements were implemented); legal issues, organization, data, systems, network, infrastructure, contingency plans, documentation, etc.

The whole questionnaire encompasses about 80 questions, which are always referenced by a specific ISO 27001 or a country/branch requirement. The auditee has to explain the practices used and to deliver material evidences to sustain his or her statements.

The questionnaire also displays the structure of the audit report. Basically, the report reflects the questionnaire's structure: Each category is evaluated according to precisely defined four maturity degrees. The whole set of maturity degrees is then consolidated to express the quality of the audit's result (not sufficient / sufficient / good / excellent). This holistic ranking enables the two pools to identify the problems faced by the individual offices, to give them the right assistance and to track the overall evolution of the corporate culture concerning the information security.

The information security audit report and the financial audit report form the most important documents to demonstrate the adherence to the governmental regulations, the agreed contractual agreements with business partners and the internal guidelines. It represents an essential document to ensure the business transparency, correctness and sustainability of this very important social institution.

The case study refers to the personal experiences of a professor who teaches Bachelor students in IT compliance and IT governance, emphasizing the topic of IT audits. On the one hand, the university requires that the foundations, the theoretical background and the research done in the topic of compliance, and particularly IT compliance are taught. On the other hand, the professor must be able to story-tell the students about the real problems arising in organizations when they implement or adjust their IT governance. The personal experiences in IT audits (in own consultancy jobs) allow the professors and the students to better reflect the conjunction between theory (research) of IT governance and its relevance (consulting) in organizations.

5. INFORMATION SECURITY FRAMEWORK

The ISO 27000 family is one of most used frameworks to design an information security concept. It encompasses three booklets ISO 2700/0/1/2. The booklet ISO 27000 introduces the main terminology and establishes a standardized language to facilitate the communication between people involved in projects related to information security. A good understanding of this vocabulary is an absolute prerequisite to further develop a consistent and enterprise specific ISMS. The students have to assimilate this set of concepts first.

The remaining booklets ISO 27001/2 encompass normative references which have to be fulfilled to obtain an ISO 27000 certification, and forty control objectives describing a set of domain requiring special attention. One hundred fourteen controls measure the degree of achievement of these control objectives. The booklet ISO 27001 describes very shortly the control objectives and the related controls, the booklet ISO 27002 explains with more details their meaning and suggests different implementation procedures. This structure is common to all different ISO norms and allows a very systematic approach for a consultant as well as for teaching tasks.

The art of a consultant resides in his or her ability to adapt the very generic contents of the ISO norm to the specific conditions which characterize the considered enterprise. He has to understand the business processes and to evaluate their inherent risks in order to interpret correctly the set of control objectives and to implement the corresponding controls.

For our specific purposes, we have developed a four-layer pyramid to best represent the hierarchy of the different levels, which constitutes an information security concept (see Fig. 1).

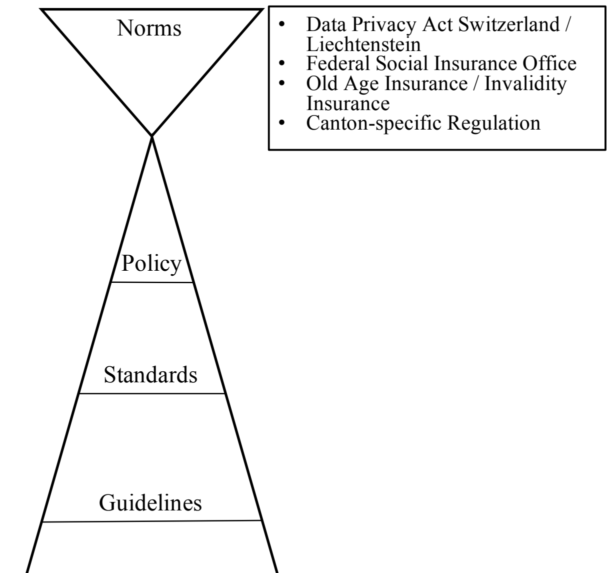
Norms
• Data Privacy Act Switzerland / Liechtenstein
• Federal Social Insurance Office
• Old Age Insurance / Invalidity Insurance
• Canton-specific Regulation
Policy
Standards
Guidelines
Procedures

Figure 1: The pyramidal or "top-to-bottom" structure of the Information Security Concept

The first layer, the Policy, assembles all the relevant laws, like the Data Privacy Act Switzerland, the Old Age Insurance and Invalidity Insurance issued by the Federal Social Insurance Office and also the whole set of Canton specific regulations. All these elements constitute the kernel of the Information Security Policy, which defines the basic elements and aims of the security concept.

The second layer, Standard, contains the different directives, and rules for Information Security and Cybercrime. These standards implement the overall Policy and formulate the minimal requirements. The adherence to the standards can be explicitly verified.

The third layer, Guidelines, gives hints to best fulfil the specifications. They consist in recommendations with wiggle room without the mandatory character of a standard. These guidelines produce most of the audit's questions.

The fourth layer, Procedures, gives instructions with binding character. They help to avoid mistakes and integrate past experiences.

This pyramid respectively pyramidal structure is projected onto a basic document "Information Security Guidelines" (ISG) which basically represents the ISMS (Information Security Management System) and a whole set of measures to implement guidelines and procedures to follow. It is segmented in ten different sections, considered as sufficient and necessary to guarantee the achievement of a satisfactory level of information security.

1) Information concerning the scope and meaning of these guidelines
2) Organization
   a) Information security organization
   b) The different roles and their description
   c) The processes
   d) Definition of protective groups for CIAT (confidentiality, integrity, availability, traceability)
   e) Risk management
3) Data
   a) Privacy data
   b) Protocols
   c) Data Management (transfer, deletion, encryption, e-mails)
4) Systems
   a) Installation and configuration
   b) Malware
   c) Systems' Monitoring
   d) Authentication and authorization
5) Network
   a) Utilization internal network
   b) Remote access
6) Infrastructure
   a) Security zones (access control and protocol)
   b) Air condition / electric generator
7) Contingency Management
   a) Buildings
   b) Data archives
   c) Restoration from networks, systems, data
   d) Disaster recovery plans
8) Documentation
   a) Mandatory documents
   b) Availability and maintenance
9) Revision
   a) Definition of standards
   b) Verification
10) Glossary

This document serves as a pattern to demonstrate how to interpret the generic ISO 27000 requirements for a specific situation. It also links appropriately the managerial dimensions of an information security concept to the underlying technology, emphasizing clearly that information security requires top priority and has to be driven by the Board. It also delivers an excellent support to consultants – and for sure to students – because most managers develop easily a certain resistance to read and interpret the somehow complex ISO jargon and prefer to have an easy understanding of how to correctly apply it.

Although, the main parts of the cantonal offices considered here do not aim to become ISO 27000 certified, all requirements listed in the ISG are referenced to this ISO norm or some other governmental regulation specific to the social insurance environment. With this referencing, we make sure that all the measures requested are rooted in field-proofed and internationally acknowledged good practices. Going systematically through the entire set of requirements addressed by ISO 27000 we also ascertain that we have not forgotten any important aspect. This explains why we consider necessary having a sufficient number of measures implemented.

6. METHODOLOGY OF THE INFORMATION SECURITY AUDIT

The audit activities consist in establishing material evidence to ascertain that the requirements listed in the ISG were correctly understood and the corresponding controls were properly implemented and are functioning accordingly. These controls are represented as paper documents, like organizational directives, checklists or they may represent some special system configurations, like password's rules, access controls to systems, data, and infrastructure.

For this, a questionnaire reflecting the same structure as the ISG was conceived. This questionnaire is being updated every year, according to the reactions and answers of the auditees, from which some questions have become obsolete, and some deserve a different wording to better explain which specific security issue was addressed. Of course the ICT environment is very dynamic and every technological move alters the dimensions susceptible to create a risk: asset, weakness and threat. In order for the audit to deliver a noticeable added-value, it is mandatory to always adapt the questionnaire to absorb these emergent security issues.

The questionnaire shows a twofold structure. The first part collects the auditee's opinions and statements. A set of pertinent questions is generated for each Information security category mentioned earlier, each question refers to an ISO 27000 requirement or control objective or to a specific regulation. The auditee is asked to explain, how the considered security issue was addressed and he or she has to hand out material evidence to back her or his statements.

Currently the whole questionnaire encompasses about 80 questions, for each question the auditee has to describe how the considered control objective was integrated in the overall compliance scheme and has to deliver material evidence to back his or her statements. The consolidation of the answers represents the substantial part of the audit report.

The filling of the second part is left to the auditor. For every question in every category the auditor has to gather enough information to decide whether the currently evaluated control objectives and controls are satisfactorily filled and whether some commentaries are necessary to validate his or her decision or if some elements are missing so that the controls are not trustworthy enough, then the couple question-answer has to be tagged with an appraisal as shown in Table 1.

Table 1: The options to validate the auditee's answers that generate either an appraisal or a commentary

<table>
<tr><th colspan="2">Category Data Thematic Scope</th></tr>
<tr><td colspan="2">The following control objectives originate from the ISG:
• Processing and transfer of personal data
• Collecting, processing and distribution of protocol data to fulfill the legal burden of proof
• General data management (transfer, deleting, encryption, child protection)
Handling of E-mails
Recovery Test for the implemented backup solution</td></tr>
<tr><td rowspan="2">⚠</td><th>Appraisal</th></tr>
<tr><td>none
F-1: Description of the appraisal</td></tr>
<tr><td rowspan="2">ℹ</td><th>Commentary</th></tr>
<tr><td>none
Description of the commentary</td></tr>
<tr><th colspan="2">Maturity Degree</th></tr>
<tr><td colspan="2">Level 1 □ Level 2 □ Level 3 □</td></tr>
</table>

The auditor then considers the whole set of questions belonging to a specific category and assigns to this category a degree of maturity. For our purposes, we have defined three different degrees of maturity as shown in Table 2.

Table 2: The defined maturity degrees

Maturity Model	
Degree	Definition
1	The processes are hardly measurable and poorly or not documented at all. The several process activities are executed on an ad hoc manner and are exclusively reactive.
2	The processes are documented and published. The documentation is not complete and its consistency is not verified. Most of the process activities are reactive.
3	The processes are documented and published. The documentation is complete and its consistency is regularly checked. The process activities are prioritized, planned and proactive.
4	Is not considered, the ratio / advantages is too bad.
5	Is not considered, the ratio / advantages is too bad.

For each tagged question-answer block the category's maturity level is downgraded to the next lower level. The next steps consist in consolidating the results obtained for each category to generate an overall estimation of the information security audit. This consolidation is ruled by the following Table 3, which shows the links between the final audit result and the different appreciations of the individual question-answer blocks.

Table 3: The classification matrix of audit

General impression	Maturity 3	Maturity 2	Maturity 1
Excellent	Min. 7	Max. 2	0
Very good	Min. 6	Max. 3	Max. 1
Good	Min. 2	Min. 4	Max. 3
Sufficient	-	Min. 5	Max. 4
Insufficient	-	< 3	> 5

Using this procedure to evaluate the overall audit presents different advantages, which allow to clearly express the added-value generated by the audit:

1) It gives the management a generic view how the security issues are handled. This is very important, because according to the Swiss laws, the management is responsible and accountable for building and maintaining an adequate level of information security. Most of the data processed by the different cantonal offices are sensitive data and any security leak will be associated with disastrous consequences for the office's management. Also, as mentioned earlier, the business processes run by the offices generate a heavy cash flow, therefore any weaknesses allowing a threat to become active have a high risk potential and must be managed and monitored according to the risk's management rules agreed by the Board.

2) These generic, office specific views may be aggregated into a comprehensive picture demonstrating the overall level of information security for the pool. It allows to define holistic measures designed to better fight against cybercrime.

3) The bottom-to-top consolidation of the whole questionnaire allows to rapidly identify which topics in which category necessitate special treatments and to prioritize their implementation.

It provides the Chief Security Officer and the Chief Risk Officer with the basic elements to structure a solid argumentation to bargain the security budget with the board.

7. RUNNING THE INFORMATION SECURITY AUDIT

The questionnaire is sent some two or three weeks before the agreed audit date, to give the information security responsible sufficient time to go through all the questions and collect the documents, he or she judges necessary to support her or his statements. The whole audit lasts one day following this program:

Phase 1 Audit Execution

1) Welcoming the participants.
2) Review of the measures related to last year's audit and their actual implementation.
3) Working on the new questionnaire. The auditee explains or legitimates his or her answer to the auditor.
4) Examination of the proposed records or documentation documents.
5) Process Checking specifically:
   a) Access right management (checking the AD)
   b) Change- and release management (verification of RfC's and the processes)
6) Technical verification:
   a) EICAR Test (this test simulates a virus attack and serves to illustrate the escalation process)
   b) Monitoring of the ICT Environment
   c) Recovery test for the implemented backup solution.
   d) Exhaustive scan of the ICT Environment (using an appropriate network analyzing tool like TNI)
7) Site inspection (server room, archive, working places)
8) Interview with randomly selected collaborators. (Data transfer, e-mails attachment)
9) Debriefing. Short presentation of some key elements identified during the audit process
10) Closing the audit's execution

Phase 2 Audit Wrap-up

1) Report's creation by the lead auditor. Basically it includes a brief summary of the audit's result, for each category an evaluation table with the commentaries, the completely answered questionnaire, for traceability reasons.
2) Report's review by the information security responsible. The auditee has the possibility to discuss the auditor's evaluation. In some cases the analysis and the appraisal or the commentaries may be adapted.
3) Validation and liberation of the report by the lead auditor. The audit report has now been finalized and has become an official status. Most of the time, it is joined with the financial audit report.

The entire audit process lasts between one and two weeks. Obviously, the audit's kernel consists in meeting the security responsible and the different checks and documents' verification. This takes one day. The elaboration of the pre-formatted report and the review depends on the availability of the requested personal resources but in about ten days the whole process should be finalized.

8. CONCLUSION

We launched the first audits series in October 2007 with seventeen cantonal offices. The corresponding results showed a strong heterogeneous picture regarding the different ways of considering the securities issues. The first audits campaign identified offices with an insufficient level of information security, most of them with a "sufficient" to "good" and very few with a "very good" one.

After three cycles all the offices had developed a sound information security awareness and only few had been ranked with "good", indeed most of them had reached the "very good" or "excellent" level.

It is remarkable, that rising through the different levels seems easier than to stay at the top. Probably it is a more rewarding task to grow out of the lower levels to reach the higher than to be strongly disciplined to maintain a high process quality. To achieve this, a large support of the Board and intensive communication are necessary. IT governance is always seeking the balance between high performance and conformance. The CSO has to legitimate processes which result in higher attention, more responsibility from each collaborator, and acceptance of controls which may appear as burdens. All this has to be to be borne by the Board, who has to be exemplary and show a seamless adherence to the agreed guidelines for information security.

One should also mention the necessity of a well-structured program, to educate the collaborators, to help them to understand the necessity of the "everyday constraints" required to care for information security. Regular training sessions and a periodical information security publication focusing on actual security topics or leaks help to maintain a high degree of acceptance for the resulting pain.

In today's business reality an adequate level of information security is absolutely mandatory. The IT enabled support to deploy the business processes efficiently is more and more invasive, some processes are completely automatized and controlled using IT based tools, and there is no way back. Information security is not trendy it has become a critical success factor for every business, therefore auditing the IT environment corresponds to ascertain the success of the business. Teaching the students has to reflect all these experiences in research and consulting in the field of IT audits.

9. REFERENCES

[1] **International Standard ISO/IEC ISO 27000/1/2**, Second Edition, 2103.

[2] T.W. Singleton, "Auditing Applications, Part 1", **ISACA Journal,** Vol. 3, 2012.

[3] T.W. Singleton, "Auditing Applications, Part 2", **ISACA Journal,** Vol. 4, 2012.

[4] E. Gelbstein, "Auditing IS/IT Risk Management, Part 1", **ISACA Journal,** Vol. 2, 2016.

[5] E. Gelbstein, "Auditing IS/IT Risk Management, Part 2", **ISACA Journal**, Vol. 3, 2016.