Implementing the ISO/IEC 17799 standard in practice – experiences on audit phases.

Timo Wiander
Department of Information Processing Science
University of Oulu
Oulu, Finland
timo.wiander@oulu.fi

Abstract

This paper introduces implementation experiences on the ISO/IEC 17799 standard. The early implementation phase showed that there was resistance to change. The study revealed that lack of information was the root cause on that. Solution for this problem is proactive communications and use of internal advocates. All interviewees shared the same view that the ISO/IEC 17799 fits well with the existing organisation culture, and even changed it to a more security conscious one. The audit phase suggested that the audit mainly supported well organisations processes and the organisations got feedback beyond audit. After the implementation phase the workload was diminished and maintenance mode was mainly seen as reasonable.

Keywords: Information Security, ISO/IEC 17799, Auditing.

1 Introduction

Global competition and global exposure to threats mean that organizations have to cover a vast variety of threats, including hacking, denial of service attacks, frauds, viruses and other malware, espionage, insider threats, social engineering and so on (Parker 1995, Im and Baskerville 2005, Whitman 2003, Theoharidou, M., Kokolakis, S., Karyda M. and Kiountouzis 2005, Barber 2001). Information security is important topic for organisations as huge amounts of information are exchanged between and within organisations. The ISO/IEC 17799 standard (2005) is widely used (Ernst & Young 2006, ISO 17799 certificates 2007) and commonly viewed as a necessary element in information security management (von Solms 2001, von Solms 1999).

However, there is no empirical evidence of the usefulness of the standard in practice. This study aims to fill this gap in the research by exploring how the practitioners perceive the ISO/IEC 17799 standard as an information security management framework. Since the standard is seen as the silver bullet of IS security management, this study contributes to the practice by critically unveiling tried and tested principles for applying IS security management standard in organisations.

Through semi-structured interviews (Eskola and Vastamäki 2001, Hirsjärvi and Hurme 2000) this study analyses the implementation experiences of four organisations that have implemented the ISO/IEC 17799 standard. The interviews took place in March 2006.

This paper has been organized as follows: Section II deals with experiences of the early implementation phase; Section III gives viewpoints on experiences on audit phases; and Section IV introduces development of the information management system after the audit. Discussion and Conclusions finish this paper.

2 Experiences of the Early Implementation Phase

During the pre-audit phase all of the interviewees mentioned that the employees viewed the information security management system process positively in general. Some parts of the discussions raised the interest of the researcher. One of the interviewees mentioned that the positive attitude lasted as long as the information security work did not affect the person in question negatively. When that happened the attitude changed to reluctance. Other interviewee told as an experience that:

> *"In the beginning the biggest surprise was that I had to win people on my side … every group had a formal or informal leader … attitude was negative if one sees that it (ISMS) brought extra work for someone … someone nagging all the time, and others are silently accepting and only a few actively supporting." (R2)*

In the case described above the interviewee had to change tactics during the implementation process. The interviewee made some effort to find the informal leaders and discuss information security issues with them. The lack of information was seemingly the root cause of resistance to change. This is also reflected in the following quote:

> *"…(employee asked) are you putting up a fascistic system? … I told that we are putting up a formalised way of working … if you apply it, you are doing the right way." (R3)*

So the uncertainty was eased with discussions and by winning the opinion leaders as advocates of the process. These findings are supported by the experiences of two interviewees who were doing the information security

management system process in a more open way regarding the communications with the personnel:

> *"… everyone understood what we were about to do, why we are doing it and what are the benefits … when people are motivated beforehand, why should they resist? … if they don't know what's coming … and they feel their own future is uncertain, then they will resist." (R4)*

This quote shows that with proactive actions the resistance to change was minimised. Table 1 formulates the finding.

Reaction	Root cause	Solution
Resistance to change. Uncertainty.	Lack of information.	Proactive communications, use of internal advocates.

Table 1: The employees' reaction to creation process, possible root cause and solutions to negative actions.

3 Experiences on Audit Phases

Typically, the interviewees looked at the upcoming audit with confidence. Four of the interviewees told almost the same story. They reserved facilities, informed the participators of who should attend to the audit and checked that the required materials, such as information security guidelines, were at hand. They skimmed through the material so that they would be able to answer any questions; otherwise, no special arrangements were made. This was the case, except in the following story:

> *"… the employees who came after the previous audit were educated quickly … quick rehearsal … checked that the minutes are OK – certain actions are done … certain matters were documented afterwards … we had to find incidents – we found them – we corrected them – got audit trail from them." (R1)*

This comment reflects that the information security process and thus the information security management system itself can get corrupted. In the sample above the organisation is seemingly only interested in keeping the certificate, the focus is not so much on the information security itself. The actions described in that case reflect that the organisation knew what the key things to do were and what to show to the auditor.

If the management are committed to the information security issues, this kind of event would not be possible. In addition, this excerpt reveals the fact that the third-party auditor can be guided in a direction that suits the auditee. On the other hand, there is limited time for conducting an audit so the real target is the management and its responsibilities. A good way for getting most out of the audit is of course to point out possible problem areas to get a real view of the current situation of the information security in the organisation, as one of the interviewees mentioned - and that even happened in the real audit situation. The interviewee perceived their information security management system, as well as their overall quality, as being so good that they wanted to get the most out of the third-party auditor by using the auditor as an evaluator of their problem areas. This approach shows that the organisations are different, even though they both have a certified information security management system.

All of the interviewees estimated that the auditor knew the special characteristics of the software industry in general, although one respondent added that the auditor did not know their business area so well. Typically, the audit went well - or as expected, as one interviewee put it - and the audit was deemed very useful. One of interviewees mentioned that the auditor was well prepared for the audit. This could be due to the fact that the auditor had done a preliminary audit on the company and had also conducted an ISO 9001 (2000) audit in that SME before. One of the interviewees raised doubts about the auditor's preparedness:

> *"… preparedness was visible … CEO told about the risk management process … it was in contrast to what was documented and the auditor did not catch it … auditor had to kind of confess the preparedness – some things we had to clarify for the auditor." (R1)*

This raises some doubts about the results and reliability of the audit. If the auditor is not well prepared (see EN ISO 19011:2002 for guidelines for executing an audit) then what are the chances of successfully conducting an audit? One must bear in mind that most of the interviewees were satisfied with the audit and the acts of the auditor. But in this particular case the auditor was not only missing the content of information security, even the process was somewhat missing. Experiences of the audit are presented in Table 2.

Index	Auditor's knowledge of software domain	Estimates of how audit was carried out	Additional information
1	+	+	Auditor was inadequately prepared.
2	+	+ +	-
3	+	+	-
4	+ +	+	Auditor was well prepared.
5	+	+	Auditor did not know the business domain.

Table 2: Experiences of the audit.

When the interviewees evaluated how the audit supported their processes, the answers varied a lot. One interviewee said that they did not dare ask anything, they were only eager to get the certificate. Two of the interviewees were positive or very positive about how the audit supported their processes. The information gathering even went so far that the auditee asked the auditor to focus on some special issues:

R: "… it is useful to hint for the auditor that here is one area where there might be some problems, could we look at this." (R2)

One of the interviewees stated that they got no direct support for the processes from the auditor or the audit itself; instead, they gained their own valuable ideas during the audit or discussion sessions. One of the interviewees mentioned that the support was rather neutral and they only got some small improvement ideas. This was said to be due to the fact that the auditor had evaluated their system beforehand and given ideas or improvement suggestions at that time and those ideas were implemented in the information security management system before the audit. A summary of the evaluations is presented in Table 3.

Index	Audit support for process	Feedback
R1	None.	Did not ask for any hints or ideas.
R2	Positive.	Got new ideas and process improvements.
R3	Directly none, indirectly yes.	No hints from the auditor; got own ideas during the audit or discussions.
R4	Very positive.	Got ideas for management and for ISO 9000 quality system.
R5	Neutral.	Got some small improvement ideas.

Table 3: How the audit supported small and medium-sized enterprises' processes and feedback beyond the audit.

The results show that the audited company gained more from the audit if they had the will. The feedback could even be beyond the scope of the audit. New improvement ideas were also generated internally, with the aid of a third-party assessor. In this respect the audits are very well reasoned.

All interviewees shared the same view that the ISO/IEC 17799 fits well with the existing organisation culture, and even changed it to a more security conscious one. The following statement reflects the interviewees' thoughts:

"Safety culture got more central status." (R2)

"… (ISO) not only fitted us, it kind of belonged to us, we just had to have it … it spurred us into doing our job even better." (R5)

"… if we think about a situation where we suddenly take the meta model away, it would be total chaos." (R1)

As a summary of the interviewees' answers, it was visible that the standard affected daily work practices positively from the information security point of view and the consequence of removal of the standard would be disastrous. A summary of the answers is presented in Table 4.

Fit to the existing culture	Impact	Consequence if removed
+ + +	Raised safety and security consciousness.	Chaotic.

Table 4: How the ISO/IEC 17799 (2005) standard affected the organisation's culture.

4 Development of the Information Management System After the Audit

After the official audit, the development efforts diminished within these organisations. Almost all of them described the situation as stabilising the situation and putting efforts to a more reasonable level after the difficult implementation phase. Says one of the interviewees:

"… we had to catch some breath." (R3)

This comment expressed the feelings of the interviewees quite well. They shared the same feeling but expressed it in different words. The implementation part was long and resource consuming. A lot of work had been done and they got the certificate as a reward for that work. The organisations changed from the development mode to the maintenance mode. The practical work hours on information security-related issues diminished but they were allocated more reasonably. For example, development efforts were concentrated on working on the remaining risks and information security-related meetings were merged into regular meetings or such minor activities. On the other hand, the new work practices were implemented so that a lot of improvements were made overall.

Only one interviewee thought the maintenance mode was seemingly harmful for the information security level. A new Information Security Officer had been nominated in that organisation. According to the interviewee, this new person was not qualified in information security and was spending most of the working hours on system development or similar issues. That situation resulted in the corruption of that particular organisation's information security management system. The management were told about the danger of that practice, and they made some modifications so that the situation was stabilised. Table 5 represents the changes within these enterprises that came up in these interviews.

Index	Change	Description	Impact
1	Maintenance	The practical work hours diminished.	Workload was balanced according the need.
2	Maintenance	Development efforts were concentrated on working on the remaining risks.	Workload was balanced according to need and the remaining risks were taken care of according to

			the business impact.
3	Maintenance	Change of work practices, for example information security-related meetings were merged into regular meetings and other small improvements were made.	More reasonable work practices implemented. Same security level with less effort.
4	Maintenance	Unified documentation.	Employees know different interfaces, procedures and guidelines better. Better documented processes.
5	Maintenance	Unqualified information security officer nominated.	The ISMS was corrupted.

Table 5: How the ISO/IEC 17799 (2005) standard affected the organisation's culture.

5 Discussion

As far as the author of this study knows, there is no empirical research available on the implementation process and results on putting the ISO/IEC 17799 standard into practice in organisations. This study is important as it reveals novel information on implementation of the ISO/IEC 17799 standard.

5.1 Limitations of the study

This study has some limitations. The sample was quite small, four Finnish organisations and five interviewed persons, so these findings might not be fully generalized. A larger sample with both domestic and international organisations could reveal more information on these issues. Furthermore, as the study focused on information security managers and their views on the standard, the study lacks the view of the management and the personnel. To give the big picture, the views of the regulators and the system auditors are needed.

The Klein and Myers (1999) criteria were used as the validation criteria. Accordingly, the validation of this research is as follows. *The principle of Contextualization*: the interviewees were asked to recollect the context and the facts surrounding the events that led to the development of their information security management system. *The principle of Interaction between the Researchers and the Subjects:* the interviews were semi-structured in nature and open questions were used, so the interviewees were allowed to provide their own interpretations of the events. *The principle of Abstraction and Generalisation:* this principle was followed by abstracting the interpretations of the cases and arguing from the particular to the general, and purposive sampling was used. *The principle of Dialogical Reasoning:* the narrative section was evolved through iterations and internal reviews. *The principle of Multiple Interpretations:* this research aimed at understanding the relationships between context and intentions, whereas power issues were not studied and social actions were in a minor role in the four organisations studied, and *the principle of Suspicion:* the data collection consisted of five interviews and four organisations, thus reducing the possible bias of one interview; control questions were used in the interviews and internal reviews were used to validate the interpretations.

5.2 Discussion of the results

Auditing proved to be useful for the organisations as the results showed. The feedback could even be beyond the scope of the audit and new improvement ideas were also generated internally, with the aid of a third-party assessor. In this respect the audits are very well reasoned.

Information security management is to be seen as a process, not a product that can be implemented in an organisation. The people and processes need constant evaluation and possibly corrective actions accordingly. The maintenance mode itself is not an issue. The interviewee mentioned that they could get more out of the information security system with fewer resources. This was because they better knew what they wanted and needed. In order to be successful, the information security work itself has to be implemented in the daily activities of the organisation. This of course calls for continuous management support. The management support is also needed for guaranteeing the successful implementation of the information security management system, as validated in the literature (von Solms. and von Solms 2004, Björk 2001).

ISO/IEC 17799 proposes a set of general requirements that are often very hard for organisations to implement. This is also the case with the other standards in full. It is important to understand that the standardisation is not necessarily needed for good information security management. And the certificate or standard itself does not guarantee the adequate information security level of an organisation.

The trustworthiness of the standard itself is an issue. ISO/IEC 17799 certification can give organisations or their interest groups a false sense of security as management or third parties could associate the "certified" or "compliant" status to mean a secure system on which no further action needs to be done. And what about the auditors – are all of them doing audits as they should be done? Within this study the auditors got quite good grades for their work. But does the same apply in every part of the world?

6 Conclusions

Information security is a necessity for all organizations, no matter what the size or industry. Building an information security management system is a great effort. To get most out of the implementation this study suggest that by using proactive communications and use of internal advocates the reluctance is diminished. All interviewees shared the same view that the ISO/IEC 17799 fits well with the existing organisation culture, and even changed it to a more security conscious one. The audit phase suggested that the audit mainly supported well organisations processes and the organisations got feedback beyond audit. After the implementation phase the workload was diminished and maintenance mode was mainly seen as reasonable.

This study aimed at analysing experiences of putting the ISO/IEC 17799 standard into practice. There are a lot to be studied though. It would be interesting to compare the experiences of auditors and auditees. Furthermore, to get the big picture, the views of the regulators and the system auditors are needed.

7 References

Parker, D.B. (1995): Using threats to demonstrate the elements of information security. *Proc. European Convention on Security and Detection on 16-18 May*: *11 – 17*. Conference publication No. **408**.

Im, G. P. and Baskerville R. L (2005): A longitudinal study of information system threat categories: the enduring problem of human error. *ACM SIGMIS Database* **36** (4): 68 – 79.

Whitman, M. E. (2003): Enemy at the gate: threats to information security. *Communications of the ACM* **46** (8): 91 - 95.

Theoharidou, M., Kokolakis, S., Karyda M. and Kiountouzis, E. (2005): The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security* **24**: 472-484.

Barber, R. (2001): Social engineering: A People Problem? *Network Security* **2001**(7):9-11.

ISO/IEC 17799. (2005): *International Organization for Standardization. Information Technology — Security Techniques — Code of Practice for Information Security Management. ISO/IEC 17799:2005(E)*. Geneva. ISO Copyright Office.

Ernst & Young: Global Information Security survey 2005. http://int.sitestat.com/ernst-and-young/international/s?Global-Information-Security-survey-2005&ns_type=pdf. Accessed 23 Aug 2006.

ISO 17799 certificates: ISO 17799 certificates world wide. http://www.iso27001certificates.com/. Accessed 26 Jun .2007.

von Solms, B (2001): Information Security – A Multidimensional Discipline. *Computers & Security* **20**:504-508.

von Solms, R. (1999): Information security management: why standards are important. *Information Management & Computer Security* **7**(1):50-58.

Eskola, J. and Vastamäki, J. (2001): *Teemahaastattelu: opit ja opetukset. (In Finnish) In: Ikkunoita tutkimusmetodeihin I. Metodin valinta ja aineiston keruu: virikkeitä aloittelevalle tutkijalle.* PS-kustannus. Gummerus kirjapaino Oy, Jyväskylä.

Hirsjärvi, S. and Hurme H. (2000): *Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. (In Finnish).* Yliopistopaino. Helsinki.

EN ISO 19011 (2002): *Guidelines for quality and/or environmental management systems auditing*. Geneva. ISO Copyright Office.

ISO/IEC 9001 (2000): ISO/IEC 9001 standard. http://www.iso.org/iso/en/iso9000-14000/understand/selection_use/selection_use.html. Accessed 16 Sep 2006.

Klein, H. K and Myers, M. D. (1999): A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly* **23**(1):67-88.

von Solms, B. and von Solms R. (2004): The 10 deadly sins of information security management. *Computers & Security* **23**(5):371-376.

Björk, F. (2001): Implementing Information Security Management Systems - An Empirical Study of Critical Success Factors. Lic thesis. Stockholm University & Royal Institute of Technology.