

ISO/IEC 17799 Standard's Intended Usage and Actual Use by the Practitioners

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

Abstract

The ISO/IEC 17799 standard (2005) is commonly viewed as a necessary element in information security management. However, there is no empirical evidence of the usefulness of the standard in practice. To study this issue, this study analyses the implementation experiences of four organisations that have implemented the ISO/IEC 17799 (2005) standard. Through semi-structured interviews, the results of the study suggest that the standard served the needs of the small and medium-sized enterprises well and its intended usage correlates quite well with small and medium-sized organisations' practice.

Keywords

ISO/IEC 17799 standard, information security management

Introduction

There are several reasons for building information security management system. Information Security Forum members (ISF 2006) have listed twelve different reasons, starting from implementation of best practice to cost savings (ISFSTD 2006). There are also several tools and methods, security guidelines, best practices, checklists and standards for building information security management systems. As we look at the standards, it is necessary to make a definition of a standard within the context of this paper:

“A standard is consensus specification resulting from an open, formal development, voting and review process.” (Isohow 2006)

According to ISO guidelines, building an information security management system consists of two standards, namely ISO/IEC 27001 (2005) and ISO/IEC 17799 (2005). Certification is done against ISO/IEC 27001 (2005), formerly known as ISO/IEC 17799 part two, which outlines the process to develop and implement an information security management system. ISO/IEC 17799 (2005) standard is the schedule of controls reflecting good practice. Both ISO/IEC 17799 (2005) and ISO/IEC 27001 (2005) provide strategic and tactical directions for implementing an information security management system. These non-technical standards recognize that information security is a management issue.

The ISO/IEC 17799 (2005) standard is based on the Code of Practice that was developed in the United Kingdom by the Department of Trade and Industry. The Code of Practice was initially published in September 1993. In 1995 the Code of Practice for Information Security Management became a British standard, BS 7799 (von Solms, 1998). The Code of Practice is argued to be based on a compilation of the best information security practices used by some large international companies, like British Oxygen, British Telecom, Shell International and Midland Bank. According to the authors, the foundation for the standard was built on real-world security actions and outlines the schedule of controls reflecting good practice (von Solms, 2000).

The ISO/IEC 17799 (2005) standard is commonly used (see e.g. Ernst & Young 2005; Xisec 2006) and its significance has been pointed out among practitioners (Tong *et al.* 2003) and cited by the academy (see e.g. Siponen 2006; von Solms 2005; von Solms 2001; von Solms 1999). And yet despite all this, there is no empirical research exploring the real usefulness of the standard in practice.

This paper aims to fill this gap in the research by exploring how the practitioners perceive the ISO/IEC 17799 (2005) standard as an information security management framework. The qualitative research method was chosen as the research method for finding answers to the research question. 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 standards in organisations.

The remainder of this paper is organised as follows: next chapter presents the research method and settings. Then the results of the interviews are presented and they are followed by discussion. Final remarks and future research questions closes the study.

Research Method and Settings

This study aims at finding out practitioners' experiences of the use and application of the ISO/IEC 17799 (2005) standard in practice. Semi-structured interviews (Hirsjärvi & Hurme 2000; Eskola & Vastamäki 2001) were used for conducting the empirical part of this work. The semi-structured interview research approach was chosen since it can capture the process nature of the phenomena and also allows revising the research plan during the entire research time (Eskola & Suoranta 2001, 15-16). The strength of the semi-structured interviews is in the richness of information, which can be obtained in real-life situations (Eskola & Suoranta 2001). This was seen as an advantage because there is no prior research on practitioners' experiences of the use of the ISO/IEC 17799 (2005) standard in practice. The *ISO/IEC 17799 standards intended usage* theme was chosen to find out how the practitioners use the standard and whether this usage actually correlated with the intended usage of the standard.

The interviews took place in March 2006. There were fifteen ISO/IEC 17799 certified organisations at that time and eight of them were chosen for interview; five small and medium-sized and three large organisations. The five people interviewed were chosen because they all had a major role in the implementation of the ISO/IEC 17799 standard and development of the information security management system within their organisations. One person from each company was interviewed, an exception being one company where two people were interviewed. This arrangement was seen as useful in order to get the full picture of the company's information security management system and its development from the ground up, because in that organisation the information security manager changed twice during the implementation process. One of the interviewed persons had also been involved in another implementation process and this gave a deeper perspective on the overall process of building an ISO/IEC 17799-compliant information security management system.

To keep the confidentiality of the interviewees it was agreed that names of the companies and people involved would be kept anonymous. Because of the small number of ISO/IEC 17799 certified companies in Finland, the researcher and interviewees agreed that the demographics of the interviewees or the companies would not be revealed, although they were discussed in the interview sessions. These limitations were seen as a necessity on the interviewees' part. To provide a general background on the interviewees, they all have been involved within information security tasks for eight or more years. Enough time for conducting interview was reserved, the interviewee controlled the time schedules and the interviewee also had the final say on where the interview was to take place. All interviews were recorded and transcribed for further study.

Analysis of the Semi-structured Interviews

One factor affecting the sufficiency of qualitative research is saturation. When the same things are repeated or no new information is gathered, saturation point is reached and the interviews may be stopped (Hirsjärvi *et al.* 1997, 180-181). Saturation could not be reliably validated in this study since there were only five interviews. In qualitative research, generalization can be formed with purposive sampling. The interviewees were selected based on their organisational role and importance in the actual development of the information security management system. There are other ways to validate the interviews. For example, Klein and Myers (1999) have laid out validation criteria for interpretations.

The interview transcripts were analyzed through three iterations to fully cover the rich qualitative content. It was also important to ensure that the concepts and findings were accurately drawn out. The first round outlined the initial themes and categories, resulting in an initial report that summarized the selected quotations and their meaning. The second round focused on these existing themes, looking for categories that clustered together, resulting in a second version of each theme with more detail and their relationships to the other themes. After this phase, internal reviews were made to validate the accuracy of the second version. Finally, the last round identified the major concepts of the findings, distilling the detail down to several specific quotations to confirm the validity and examples that validated the core themes and ideas as represented in the interviews. This study is the output of this process, and the themes are finally in a format that would answer the research question.

Interview Results

The interviewed companies also considered other frameworks. The ISF (2006) was mentioned as an alternative, but it was not used since it was too expensive, said one interviewee. Furthermore, the ISF (2006) was seen as too difficult to implement because it did not downscale for that small organisation's purposes:

R: "(ISF) why we didn't take that ... first of all, it was about the costs and the secondary reason was that the model... from my point of view... it was visible that the model was good for the mega-sized organisations ...how well does it scale downwards, that's a different story." (R4)

The costs and the suitability of the model are important factors when choosing a framework for information security, as shown by the sample above. The scalability of the model is another issue for small and medium-sized organisations. Two interviewees mentioned the ISO 9000 (2000) series as an alternative, but as it is a quality management system rather than an information security management system, it was not implemented. GASSP (2006) was also mentioned, as well as SSE-CMM (2006). One of interviewees stated that there were no alternative frameworks considered because they had decided to go for ISO/IEC 17799 (2005).

ISO/IEC 17799 Standard's Intended Usage and Actual Use by the Practitioners

According to ISO (Isousage 2006), the standard is suitable for several different types of use and information was gathered to evaluate how the practitioners viewed the issues ISO organisation argues to be valid for choosing the standard and whether the standard was used as it was meant to be. The results are presented in Table 1.

Table 1: The intended and the actual use of the ISO/IEC 17799 (2005) standard

Index	Item	Used by
1	Formulate security requirements and objectives.	5
2	To ensure that security risks are cost-effectively managed.	4
3	To ensure compliance with laws and regulations.	4
4	A process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met.	5
5	Definition of new information security management processes.	5
6	Identification and clarification of existing information security management processes.	5
7	Determination of the status of information security management activities.	5
8	Use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization.	5
9	Use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons.	5
10	Implementation of business-enabling information security.	3
11	Use by organizations to provide relevant information about information security to customers.	5

The standard was used to *formulate security requirements and objectives* by all of the organisations. Different risk analysis tools and methods were used. For example, POA (2006), risk scenarios, scenario analysis, fault tree analysis and organisations' own risk assessment Excel sheets were mentioned. Furthermore, laws and statutes, regulator requirements, business agreements and customer requirements set their demands for the information security management system. The organisations also used their internal tools, such as safety policies, and gathered their own and business units' expectations of the system. Common sense was mentioned too. Usage of the standard to *ensure that security risks are cost-effectively managed* was also found true since only one interviewee mentioned that the costs were not monitored; in that particular case it was important to get the standard for marketing reasons.

Evidence was gathered on how the ISO/IEC 17799 (2005) standard was used to *ensure compliance with laws and regulations*. This proved to be true. All except one mentioned that the compliance with law and regulations was an issue. One even mentioned that they have to align with different laws in other countries as well. The Finnish Vahti (2006) documentation was also mentioned as guidelines. The instructions were integrated into the Information Security Management System. Through the interviews it became quite clear that the ISO/IEC 17799 (2005) standard was used as a *process framework*. The standard was found helpful for *defining information security management processes* and *in identification and clarification of existing information security management processes* by all of the interviewees. Two of the interviewees mentioned that the process definition

was taken from a textbook and further developed during the implementation process. The interviewees also mentioned that there were processes concerning the technical information security issues before. A more holistic view of the information security and the actual management process came with the implementation of the ISO/IEC 17799 (2005) standard. One of the interviewees mentioned that the existing safety processes were further developed to cover the information security issues and one of the interviewees mentioned that they implemented the safety practices of Yritysturvallisuuden neuvottelukunta (YTNK 2006).

On the *determination of the status of information security management activities* all interviewees confirmed that the standard gave them the means for reporting the information security activities, for example incidents and risk assessments, for management. Within these small and medium-sized organisations the typical case was that the management was aware of even small details concerning the security on an almost daily basis. The reporting was typically based on the needs of management and included structured (written reports and e-mails) and unstructured means (discussions). One of the interviewees criticised the reporting for being meant only for holding the certificate, for example audit trail and constant development issues were covered, and there was no true effort made to dig deeper into the real problems.

Because all of the organisations within this study held a certificate it was clear that *the standard was used by internal and external parties to determine the degree of compliance issues*. A typical method for gathering information was checklists. Technical audits were also made; for example password crackers were used. Typically, the internal auditor was the security officer. In one case the audits were done by the quality assurance department. The audits were typically made to fulfil the requirement of the standard. According to International Organization for Standardization (Isousage 2006), the standard itself could be used for *providing relevant information about information security issues to third parties*. This was found to be true. The interest groups were informed direct, for example using e-mails. Indirect media such as the Internet were also mentioned, as well as using consult's information distribution channels. The information distribution was not always successful as one of the interviewees mentioned that they wrote a press release but it did not catch any publicity. The interviewee thought that this might be due to the certification of a larger organisation at the same time.

The claim that the ISO/IEC 17799 (2005) standard could be used for *implementation of business-enabling information security* was supported by three interviewees. The interviewees perceived that the information security role was to be a supportive action. The most critical dimensions for these organisations were profitability, continuity of business and personnel. Other mentioned issues were trust, quality and reputation. As the last case evidence on how these organisations used the ISO/IEC 17799 (2005) standard as a tool for *providing relevant information about information security to customers*, all of the interviewees mentioned that this is true. It became clear that the certificate also has a selling point status. The message they wanted to give to their customers was that the organisation takes information security seriously and that they invest in it. Building reputation was also mentioned. One organisation wanted the standard because they wanted to look bigger than they are. In summary it can be stated that the ISO/IEC 17799 (2005) standard served the needs of the small and medium-sized enterprises well and its intended usage correlates quite well with small and medium-sized organisations' practice.

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 (2005) standard into practice in organisations. This study aimed to fill this gap in the research by exploring how the practitioners perceive the ISO/IEC 17799 (2005) standard as an information security management framework. This study is important as it reveals novel information on implementation of the ISO/IEC 17799 (2005) standard. The results are based on the answers from five people who all had a major role in the implementation of the ISO/IEC 17799 standard and development of the information security management system within small and medium-sized organisations. The small and medium-sized organisations employ high numbers of personnel, and their significance is recognised (EU, 2005). In our networked world the companies form long chains of clients and subcontracting organisations, whose level of information security is an issue.

This study has some limitations. The sample was quite small, four Finnish small and medium-sized 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.

Discussion of the Results

The early versions of the standard had strict emphasis on applying all the key controls. This, and the fact that the creation process of the standard has not been transparent, has raised criticism. Siponen (2005, 341) argues that security management standards violate Hume's law in implementing what organisations should do as opposed to what it is possible to do. This is especially the case with the older versions of the ISO/IEC 17799 standards. Siponen (2005, 341) continues that information security standards substitute an organisation's unique information security requirements. The new ISO/IEC 27001 has moved further away from this drawback by emphasising the organisation's own risk assessment as the point of departure.

These practitioners evaluated the ISO/IEC 17799 (2005) standard as offering a trustworthy security framework. It offers a risk-based approach to information security and could be utilised in risk management, even though the standard is not a dedicated tool for handling risks. Furthermore, the standard pushes the organisations to clarify the processes and make better documentation. Thus the risks related to assets, whether people (losing key personnel or frauds) or data (forgeries), are diminished. The standard gives guidelines on how to protect sensitive information, yet leaves a lot of room for the actual implementation of the controls. The interviewees also perceived that the implementation of the standard changed the whole way of working towards a more secure way of practising it. This means that the client actually benefits from the implementation of the standard too. And, according to the interviewees, these small and medium-sized organisations gained from the new information security processes as well. Ideally, this new and good work practice is incorporated in day-to-day actions. This of course calls for continuous management support. The management support is also needed for guaranteeing the successful implementation of the process, as validated in the literature (von Solms & von Solms, 2004; Björk, 2006). The ISO/IEC 17799 (2005) standard itself emphasises a continuous improvement process, which forces organisations to always think about security and the risks involved in doing business.

The interviewees mentioned that they used the ISO/IEC 17799 (2005) standard as a source when making their information security management system and the information security policy. Baskerville and Siponen (2002, 338) have stated that using generic standards as a basis for security policy development has several shortcomings. They listed four cases: 1) generic standards do not pay adequate attention to the fact that organizations differ, and therefore their security requirements will differ; 2) generic standards do not take into account the social nature of the problems; 3) generic standards overlook the normal business requirements of organizations and as a result a conflict between the organization's normal business requirements and security requirements proposed by security standards may arise; and 4) generic standards are broadly written necessitating ad hoc managerial decision making and judgment. Baskerville and Siponen (2002, 338) also expressed the opinion that the generic standards do not provide any help concerning these decision-making problems. One striking comment in this study was that one organisation not only took a sample policy, they found that policy document so useful that they committed to what was written.

The trustworthiness of the standard itself is an issue. ISO/IEC 17799 (2005) 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. The new ISO/IEC 17799 (2005) standard is not strict on the implementation of the controls, as the following excerpt shows: "This code of practice may be regarded as a starting point for developing organization specific guidelines." and it continues: "Not all of the controls and guidance in this code of practice may be applicable." (ISO/IEC 17799 2005, 11). The ISO/IEC 17799 (2005) standard leaves room for organisations' own guidelines and controls by stating: "Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners." (ISO/IEC 17799 2005, 11). These are good intentions but are they acting as solid guidelines? The small and medium-sized organisations proposed that the ISO organisation could make guidelines and mappings of the safety functions as a starting point.

All these reflect that there is a need for a more agile framework for implementing the ISO/IEC 17799 (2005) standard in practice. Perhaps by combining the agile methods with the development of the information security management system we could have a new approach to the actual information security management work?

Conclusion

The ISO/IEC 17799 standard (2005) is commonly viewed as a necessary element in information security management. However, there is no empirical evidence of the usefulness of the standard in practice. To study this issue, this study analysed the implementation experiences of four organisations that have implemented the ISO/IEC 17799 (2005) standard. Through semi-structured interviews, the results of the study suggest that the standard served the needs of the small and medium-sized enterprises well and its intended usage correlates quite well with small and medium-sized organisations' practice.

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 find out whether there any practices in use that are totally missing in the ISO/IEC 17799 standard? Furthermore, it would be interesting to find out how to combine agile methods and the development of an information security management system so that a tailor-made information security management system based on the actual risks of an organisation can be built.

References

- Baskerville, R. & Siponen, M.T. 2002, 'An Information Security Meta-policy for Emergent Organizations'. *Journal of Logistics Information Management, special issue on Information Security*, vol. 5-6, pp. 337-346.
- Björk, F. 2006, *Implementing Information Security Management Systems - An Empirical Study of Critical Success Factors*, viewed 7.9.2006 <<http://www.dsv.su.se/~bjorck/files/bjorck-thesis.pdf#search=%22security%20scandinavian%20style%22>>
- Eskola, J. & Suoranta, J. 2001, *Johdatus laadulliseen tutkimukseen*. (In Finnish). Vastapaino. Jyväskylä.
- Eskola, J. & 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.
- Ernst & Young. 2005, *Global Information Security survey 2005*, viewed 23.8.2006 <http://int.sitestat.com/ernst-and-young/international/s?Global-Information-Security-survey-2005&ns_type=pdf>.
- EU. 2005, *SME definition*, viewed 22.8.2006 <http://europa.eu.int/comm/enterprise/enterprise_policy/sme_definition/index_en.htm>.
- GASSP. 2006, *Generally Accepted System Security Principles*, viewed 13.9.2006 <http://www.issa.org/gaisp/_pdfs/v30.pdf>.
- Hirsjärvi, S. & Hurme, H. 2000, *Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö*. (In Finnish). Yliopistopaino. Helsinki.
- ISF. 2006, *Information Security Forum*, viewed 22.6.2006 <<http://www.securityforum.org/html/frameset.htm>>.
- ISFSTD. 2006, *Information Security Forum. The Standard of Good Practice for Information Security*, viewed 25.8.2006 <http://www.isfsecuritystandard.com/index_ns.htm>.
- ISO/IEC 17799. 2005, *ISO/IEC 17799:2005(E). International Organization for Standardization. Information Technology — Security Techniques — Code of Practice for Information Security Management*. Geneva. ISO Copyright Office.
- ISO/IEC 27001. 2005, *International Organization for Standardization. Information Technology — Security Techniques — Information security management systems — Requirements*. Geneva. ISO Copyright Office.
- ISOHOW. 2006, *Who, when and how – development of the ISO standards*, viewed 1.9.2006 <<http://www.iso.org/iso/en/stdsdevelopment/whowhenhow/how.html>>.
- ISOUSAGE. 2006, *ISO standards intended usage*, viewed 1.9.2006 <<http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103&ICS1=35&ICS2=40&ICS3=>>>.
- Klein, H. K & Myers, M. D. 1999, 'A set of principles for conducting and evaluating interpretive field studies in information systems', *MIS Quarterly* vol. 23, issue 1, pp. 67-88.

- POA. 2006, *Potentiaalisten ongelmien analyysi* (In Finnish; Analysis of potential risks), viewed 3.9.2006 <<http://www.pk-rh.com/en/index.html>>.
- Siponen, M. T. 2005, 'Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods' *Information and Organization* vol. 15, issue 4, pp. 339 – 375.
- Siponen, M.T. 2006, 'Information Security Standards Focus on the Existence of Process, Not Its Content?' *Communications of the ACM* vol. 49, issue 8, pp. 97 – 100.
- von Solms, B. 2000, 'Information Security – The Third Wave?' *Computers & Security* vol. 19, pp. 615 – 620.
- von Solms, B. 2001, 'Information Security – A Multidimensional Discipline' *Computers & Security* vol. 20, pp. 504-508.
- von Solms, B. 2005, 'Information Security governance: COBIT or ISO 17799 or both?' *Computers & Security* vol. 24, pp. 99-104.
- von Solms, B. & von Solms R. 2004, 'The 10 deadly sins of information security management' *Computers & Security* vol. 23, Issue 5, pp. 371-376.
- von Solms, R. 1998, 'Information security management (3): the Code of Practice for Information Security Management (BS 7799)' *Information Management & Computer Security* vol. 6, Issue 5, pp. 224–225.
- von Solms, R. 1999, 'Information security management: why standards are important' *Information Management & Computer Security* vol. 7, Issue 1, pp. 50-58.
- SSE-CMM. 2006, *Systems Security Engineering Capability Maturity Model. The International Systems Security Engineering Association*, viewed 25.1.2006 <<http://www.sse-cmm.org/>>.
- Tong, C. K. S., Fung, K. H., Huang, H. Y. H. & Chan, K. K. 2003, 'Implementation of ISO17799 and BS7799 in picture archiving and communication system: local experience in implementation of BS7799 standard.' *International Congress Series*.
- Vahti. 2006, *Valtionhallinnon tietoturvallisuuden johtoryhmä* (in Finnish; *The Finnish government information security management board*) viewed 3.9.2006 <www.vm.fi/tietoturvallisuus>.
- YTNK. 2006, *Yritysturvallisuuden neuvottelukunta* (in Finnish; *The consultative committee for corporate security, a joint organisation of the Confederation of Finnish Industries, shortened as EK in Finnish and its member unions and companies*), viewed 3.9.2006 <<http://www.ek.fi/ytnk/yritysturvallisuus/index.php>>.

Copyright

Timo Wiander © 2007. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.