A Cluster Approach to Security Improvement according to ISO/IEC 27001

Nicolas Mayer
Centre de Recherche Public Henri Tudor
29 av. John F. Kennedy, L-1855 Luxembourg
nicolas.mayer@tudor.lu

Abstract

ISO/IEC 27001 is currently the standard approach to Information System (IS) security. It explains how to establish an Information Security Management System (ISMS) which objective is a continual improvement of information security. The associated certification is an evidence for the stakeholders of the organisation that security risks are assessed and treated. However, this standard is still considered as difficult to implement by SMEs, mainly due to their limited financial and human resources. It is generally a costly process until being certified and a deep knowledge of the standard and its principles is required. In order to consider this issue, we developed within a research project an implementation guide, templates and software tools to assist SMEs in ISMS establishment. This paper presents the validation of these results through industrial experimentations in three different organisations.

Keywords

information security, ISO/IEC 27001, compliance, SME

1 Introduction and problem statement

Information security is at the heart of Information Systems (IS). For example, in the past two years, 52% of businesses have experienced an unforeseen interruption, and the vast majority (81%) of these interruptions has caused the business to be closed for one or more days [1]. A challenge of today remains that security should be adapted to each organisation. Each organisation should select security measures that are suited to its security needs, instead of trying to target an unreachable level of security. In this context, the ISO/IEC 27001 standard [2] is a suited answer. The objective of the standard is a continuous improvement of information security. This continuous improvement is provided through the establishment and management of an Information Security Management System (ISMS). An ISMS involves especially that a risk management approach has been used to assess the security of the organisation, and thus that relevant measures have been selected and implemented. An ISMS of an organisation can be certified, in order to give some confidence to stakeholders that the ISMS is compliant with the standard and, therefore, that a continuous improvement of information security is guaranteed.

A key characteristic of the ISO/IEC 27001 standard is that it covers all types of organisations, irrespective of its size, origin or activity. Based on our previous work [3], an SME has some strength regarding the adoption of the principles of the standard, like flexibility and reactivity. However, they have also a main issue regarding the establishment of an ISMS: their limited financial and human resources. The establishment of an ISMS is most often a long and costly process, and it needs to involve people with a good knowledge of the standard.

The objective of our research work is to help SMEs to adopt the ISO/IEC 27001 standard, through the improvement of the ISMS establishment process. This paper is about the experiments of our research results in this field with different SMEs. Section 2 of the paper briefly presents the ISO/IEC 27001 standard. Then, Section 3 summarises our research results for ISMS establishment. Section 4 is about the two experiments performed and it reports the lessons learned. Finally, Section 5 draws the conclusion of these experiments and describes the future work.

2 The ISO/IEC 27001 standard

The outcome of ISO/IEC 27001 [2] is the effective establishment and management of an ISMS. The purpose is a continual improvement of information security. Relying upon quality management and ISO 9001 [4] principles, the standard is built around a PDCA (Plan-Do-Check-Act) cycle. It is necessary to note that the standard does not require nor induce an absolute level of security to reach. The objective is to ensure a constant alignment to the organisation security needs and to improve security over time. This objective is reached through the use of a risk management approach. It aims at selecting and implementing security measures that are suited to the security risks of the organisation.

The standard contains a set of normative requirements one must comply with to obtain the certification. They are expressed from Section 4 to Section 8 of the standard (see Figure 1) and also include Appendix A. The other sections are considered as informative, and thus are not mandatory for the certification.

It is necessary to establish and manage the ISMS by following the PDCA cycle composed of four iterative steps (described from Section 4.2.1 to Section 4.2.4 in the standard). The whole ISMS must be supported by a specific documentation, whose requirements are explained in Section 4.3. Additionally, some requirements are especially developed in a dedicated section, because of their importance or complexity. Thus, the standard includes sections regarding management responsibility (Section 5), internal ISMS audits (Section 6), management review of the ISMS (Section 7) and ISMS improvement (Section 8).

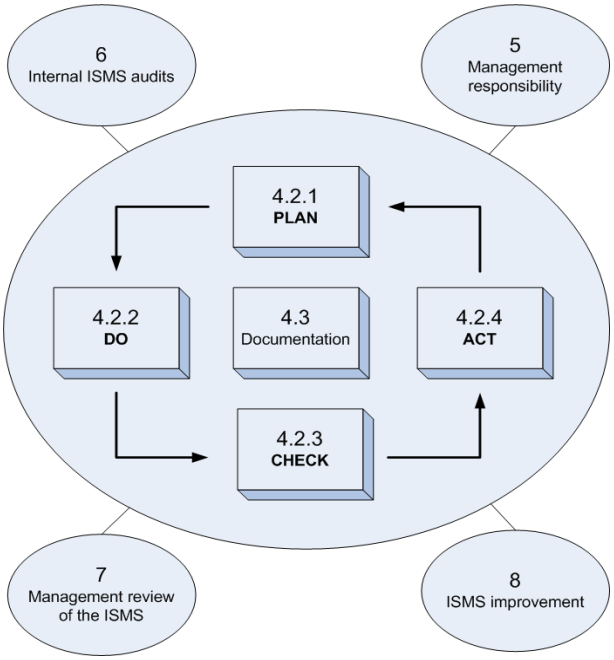

Figure 1: Representation of the ISO/IEC 27001 standard

Moreover, the standard requires to assess the selection of the security measures listed in Appendix A. This selection is performed and justified in a document called "Statement of Applicability". Appendix A consists of a list of 133 security controls, based on ISO/IEC 27002 [5]. Those controls cover the complete scope of information security, by providing IT technical measures (e.g., system acceptance, protection against malicious code), management measures (e.g., security policy, business continuity planning), measures on physical security (e.g., secure areas, equipment security) and human resources security (e.g., security awareness, termination or change of employment).

3 Research results for ISMS establishment

The industrial experience report described in this paper is based on a previous research project [3]. The objective is now to assess and validate the results in an industrial context. The above mentioned project aims at identifying what are the specific needs of SMEs regarding ISMS, and how to establish an ISMS in an SME context. The outcomes of this project are 1) an implementation guide taking into account the specificities of SMEs, 2) templates and software tools supporting the implementation process described in the guide. In order to develop these artefacts in a structured way, we propose a research method following an action research approach [6]. The research method, presented in Figure 2, consists of three steps:

- **Step 1** – *Initial experiment*: An initial experiment of ISMS implementation in an SME context is performed, in order to identify the related issues.
- **Step 2** – *Building the guide and the templates*: The guide and the supporting templates and tools are developed based on the conclusions drawn during step 1. They are then reviewed by experts, in order to have a first level of validation.
- **Step 3** – *Experimenting the guide*: In order to strengthen the validation, industrial experiments are conducted.

It is necessary to note that Step 2 and 3 are performed iteratively, with incremental updates of the results. Step 1 and 2 are currently finished. Two expert review processes have been performed in Step 2. The two experiments planned for Step 3 are also finished and are the topic of this paper.

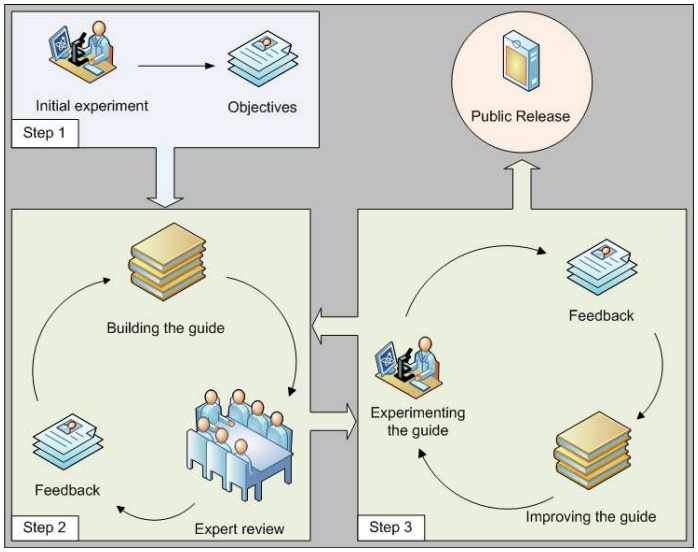

Figure 2: Research method of the project

4 Experiments

Two experiments were conducted in order to assess our research results. The first one was an experiment on a single organisation. The objective was to test our results (the guide, the templates and the tools) in a classical frame, through the establishment of an ISMS. The second one was more innovative, because we tested our results on a cluster composed of two organisations. After assessing the effectiveness of our research results in the first experiment, the objective was then to assess their efficiency in the second, by constraining the time and effort needed to establish the ISMS in both organisations.

4.1 Assessment of our research results with a single company

The first experiment took place in the Luxembourg's Ministry of the Economy and Foreign Trade (MEFT). The scope was not the whole MEFT, but only two departments. The first one was the Human Resources (HR) department and the second one was the department in charge of IT management and management of the national website about information security (http://www.cases.lu). The experiment started in April 2009 and ended in December 2009. The project team of the MEFT was composed of the leader of the HR department, two persons involved in the IT management and two persons involved in the website management. The objective of establishing an ISMS for the MEFT was to improve security management in these two key departments.

This experiment had an interesting initial context. The team had already a good knowledge about information security and the ISO/IEC 27001 standard. A risk assessment had already been done in 2006 with the EBIOS method [7]. Moreover, a security policy and some of the key procedures necessary for an ISMS were already defined, like incident management or control of documents. Finally, the security level of the organisation was already good and many security measures recommended in the appendix of the standard were already implemented.

The experiment work plan was composed of the following steps:

- Initial training about the ISO/IEC 27001 standard and our implementation guide;
- Gap analysis between the current state and the state-to-be;

- Update of existing procedures, based on our templates and tools;
- Definition of missing procedures, based on our templates and tools;
- ISMS validation;
- Management review of the ISMS.

The experiment is currently finished. The positive aspects in this experiment were the competence of people involved in the project. There were also some weaknesses mainly related to the availability of the team. This lack of availability implied that we were not able to completely perform our work plan. However, it was an interesting experiment, giving some interesting feedback to validate our results, as described in Section 4.3. It helped to strengthen our implementation guide and the associated templates. It was also a good way to validate the usefulness of the software tools we used during the gap analysis and the risk management steps.

4.2 A cluster approach to ISMS establishment

In this experiment, the innovation is in the cluster approach to ISMS establishment. In this context, a cluster is defined as the composition of a group of organisations wanting to implement the ISO/IEC 27001 standard. In our context, two companies form the cluster. Our assumption is that an efficient cluster should be composed from three to five organisations (see Section 5). However, in order to mitigate the risk related to this cluster experiment, and in order to respect the time and budget constraints of our research project, we restricted the cluster to two organisations for this experiment. The first interest of a cluster approach to ISMS establishment is the reduction of the associated cost. The cost of the trainings are supported by the whole cluster and thus divided by the number of organisations within the cluster. Another strength of the cluster approach is that the organisations can share their feedback about ISMS establishment. In each training session, some time is dedicated to this activity.

Some criteria are defined to well scope the organisations that can join the cluster:

- The organisation must be a small or very small enterprise. The total length of our approach and the different steps are sized for SMEs.
- The management commitment for ISMS establishment is a fundamental prerequisite. Without such a commitment prior to the beginning of the project, the risk of giving up during the project remains too high.
- The availability of enough human and financial resources must also be clear prior to the beginning of the project.

The cluster approach is composed of three parts. The first one is a gap analysis of half a day on site and half a day of result analysis. The second part is a training of 6,5 days, including an initial training of 1,5 days. The training is divided in sessions, most often on a half day basis. Finally, the third part of the approach is the individual coaching of each organisation. The coaching part consists of half-days of help to implementation, review and validation of the work done. The number of necessary coaching is different from one organisation to another. It depends on the competencies of the organisation, and on the work already done before the beginning of the cluster we can reuse for the ISMS. A coarse-grained estimation of this charge can be done through the gap analysis. We evaluate the coaching ceiling at 14 days.

The work plan of this experiment is:

- Planning definition;
- Initial training about the ISO/IEC 27001 standard and our implementation guide;
- Gap analysis between the current state and the state-to-be;
- Succession of “training / associated coaching” cycles on a 3-4 weeks basis.

For the training part, we need to divide the standard in coherent sets of requirements. The objective is to structure the trainings on a half day basis, in order to avoid to give too much information during each training session to the attendees. During trainings, each attendee shall learn a limited number of knowledge, he shall be able to apply during the weeks following the trainings. Moreover, the focus of these trainings is put on know-how needed by the attendees, like how to use our tools or templates. Most of the theoretical knowledge is learned during the initial training. It is highly recommended for each organisation to have two persons following the trainings, in order to have a backup for the different steps of the ISMS establishment. The trainings are:

- Scope, ISMS policy and assets (0.5d);
- Risk assessment (0.5d);
- Risk treatment and treatment plan (0.5d);
- Document management (0.5d);
- Security policy, security measures and effectiveness (2 x 0.5d);
- Human resources management (0.5d);
- Incident management and continual improvement (0.5d);
- Management review of the ISMS (0.5d);
- Audit (0.5d).

The first company in the cluster is IfOnline. IfOnline manages the IS of a building in Luxembourg, shared mainly by financial organisations. Its second activity is service provider for a HR software. IfOnline is a very small enterprise of four employees. The IS security of IfOnline is regularly audited. The objective of IfOnline is to be certified in order to reduce the length and scope of these audits. The project team is composed of a manager of IfOnline and a second employee. The scope of the certification is the whole organisation of IfOnline. The second organisation of the cluster is the Luxembourg Airport Authority (LAA). The LAA has many missions like the air traffic control under Luxembourg jurisdiction, the management of aeronautical telecommunications exchanges, the meteorological assistance to air traffic as well as international cooperation concerning climatology, etc. The LAA is an organisation of about 150 employees. Four persons composed the project team. A project manager was in charge of the project, and he was supported by three persons: two from the IT department and the physical security manager of the LAA. The LAA must comply with the European commission regulation No 2096/2005 laying down common requirements for the provision of air navigation services. A requirement of this regulation is to have a security management system established, especially in order to ensure “the security of operational data it receives or produces [...], so that access to it is restricted only to those authorised”. An ISO/IEC 27001 certification is thus a suited answer to satisfy this requirement. The scope for LAA is initially the administrative department, and will be extended in a second step to the whole organisation. The experiment started with the two organisations in October 2009 and will finish in April 2010.

The initial context of IfOnline is a good security and awareness level, because security is at the core of their business. Many recommended security controls are already in place. However, there is a lack at the documentation level and most of the controls are very few formalised. For the LAA, the initial context is different. They are already ISO/IEC 9001 certified [3] and thus many mandatory procedures are already existing (audit, management review, document management, etc.). A risk assessment focused on physical security has already been performed. The LAA shall mainly improve its information security, based on a complete risk assessment.

The experiment is currently finished, and both organisations are preparing the certification. For IfOnline, the ISMS is currently established in the whole organisation and the certification audit is planned for the last quarter of 2010. Regarding the LAA, some security measures in the administrative department are still missing. They are currently implemented in order to complete the ISMS establishment. From the third quarter of 2010, they will start to extend the ISMS scope to the whole LAA. They expect to be certified in 2011.

4.3 Lessons learned

For the first experiment with the MEFT, the guide and the associated tools were a reference helping to highlight the strength and weaknesses of the procedures and practices in use. For example, after presenting the documentation requirements of the standard and our implementation proposal, the conclusion was that our approach is more suited to the MEFT than their existing procedure. A second example is about the risk assessment approach. The review of the risk assessment was performed based on the results of the previous one. However, the method used was modified, and the data were gathered thanks to our software tool. This feedback reinforces the need to keep simple an ISMS and to propose examples that are suitable to SMEs. The second main observation of this experiment was the key motivation provided by the certification constraint. This point was missing in this experiment, because the testing of this new approach was the main objective for the MEFT, and not the certification. The certification encompasses some pressure coming especially from the deadlines imposed by the audits. When the certification is not an objective for the organisation, it is difficult to keep the pressure on the team. As a conclusion, even the experiment was not fully completed, the feedback from the MEFT is good, because the result is 1) a better understanding of the standard, its requirements and its setting up by the whole team, 2) an improvement of the procedures already in place, and 3) the update of their risk assessment, showing some remaining gaps in security and which new procedure and/or practice shall be put in place.

For the cluster approach, the difference between both organisations was very interesting for validation purpose (e.g., public/private, number of employees, activities, etc.). It showed that our package is suited to different SME's contexts. It was first interesting to observe that both organisations did not have any problem to speak about their feedback all along the experiment. Although we had some doubts at the beginning of the project about the opportunity to have open discussions between the organisations about their ISMS, they were not impervious to information exchange. This point was reinforced by the fact that the organisations were not rivals, working on the same market. Their feedback about this aspect of experience sharing was very positive. Then, the planning definition is a key step for the cluster approach. It is necessary to define at the beginning of the project a planning taking into account the potential unavailability or overloaded periods for the different organisation, in order to avoid that an organisation has some late. A continual progress of each organisation all along the project is necessary. Our initial planning took into account these unavailability periods and it was a success factor. Regarding the tools and templates, the feedback was first that they have more added-value with a low-maturity organisation. Naturally, an organisation already ISO/IEC 9001 certified will not use every templates of the package. However, even in this context, the efficiency of establishing an ISMS with our package is better than without any support. Time consumed for establishing an ISMS in this experiment was about a third of time consumed in the initial experiment of the project [8]. Finally, based on the feedback gathered, the most interesting aspect of this experiment was the model of the training part. The division of the training in half-day sessions and the mix between theoretical aspects, mainly learned during the initial training, and practical ones, during training sessions, was the key aspect of our model. The LAA and IfOnline confirmed that it is a cornerstone for an efficient progress all along the project.

At least, both experiments were the input for the next step of our project that is the transfer of the research results to SMEs and consulting firms. The objective is now to train professionals to establish an ISMS with our tools. A labelling scheme is currently defined. The label shall guarantee that its owner is able to provide an accompaniment to a SME all along its ISMS establishment. Each person wanting to obtain the label must first follow a training, then pass the associated exam and finally be evaluated by a coach during its first ISMS establishment mission. For the last part about evaluation by a coach during a concrete mission, the experience collected during our experiments provides us most of the requirements. The requirements shall reflect the different skills one must have to be effective during the mission. These requirements are organised into four categories reflecting the different parts of the accompaniment:

- Gap analysis
- Risk management
- Management system procedures

- Security policies and procedures

5 Conclusion and future work

This paper reports about the two experiments conducted in the frame of a research project [3] about the ISO/IEC 27001 standard in an SME context. The experiments aim at validating the research results of the project: a guide, templates and software tools that form a package for supporting the ISMS establishment in SMEs. The first experiment was the use of this package for establishing an ISMS in two departments of the MEFT. The second experiment was a cluster approach to ISMS establishment, performed with two organisations: IfOnline and the LAA.

The conclusion drawn from the experiments are first that our package is relevant for an SME. As explained in Section 4.3, the time needed for ISMS establishment is shorter with our tools than without. Moreover, the collective aspects of the cluster approach have shown their interests. More interesting, some SMEs acknowledge than without our package and our cluster approach, they would not be able to target ISO/IEC 27001 certification. It is necessary to note that a new cluster of 4 organisations shall start in the second quarter of 2010. The global objective of demonstrating to SMEs that they can establish an ISMS in a simple and efficient manner and that they can target the certification is reached.

Current work is about the transfer of our tools. A strategy is currently defined, in order to transfer to consulting firm and SMEs our package. A way of transfer we also consider is to start new clusters in which we deliver the training part and some consulting firms provide the coaching part. Finally, feedbacks in general on ISO/IEC 27001 in SMEs are positive and spur ourselves on going on in this way. The first private SME ISO/IEC 27001 certified in Luxembourg announced recently that their break-even point for the certification will occur three years after their certification.

6 Literature

1. Agility Recovery Solutions, Hughes Marketing Group. 2009. Disaster Recovery & Business Continuity Survey.
2. ISO/IEC 27001. Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization, Geneva, 2005.
3. Thierry Valdevit, Nicolas Mayer, and Béatrix Barafort. Tailoring ISO/IEC 27001 for SMEs : A Guide to Implement an Information Security Management System in Small Settings. In Springer, editor, Proceedings of the 16th European Systems & Software Process Improvement and Innovation Conference (EUROSPI'09), 2009.
4. ISO 9001. Quality management systems - Requirements. International Organization for Standardization, Geneva, 2000.
5. ISO/IEC 27002. Information technology - Security techniques - Code of practice for information security management. International Organization for Standardization, Geneva, 2005.
6. David E. Avison, Francis Lau, Michael D. Myers, and Peter Axel Nielsen. Action research. Commun. ACM, 42(1):94-97, 1999.
7. DCSSI. EBIOS - Expression of Needs and Identification of Security Objectives. http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html, France, 2004.
8. Nicolas Mayer. Model-based Management of Information System Security Risk. PhD thesis, University of Namur, 2009.

7 Author CVs

Nicolas Mayer received his M.Sc. degree from the University Henri Poincaré, Nancy, France, in 2004, and his Ph.D. degree from the University of Namur, Belgium, in 2009. He is currently product manager at the CRP Henri Tudor, Luxembourg, for the business line "Security & continuity management". His research interests are mainly in the fields of risk management, IS security and requirements engineering.