A GAP ANALYSIS TOOL FOR SMES TARGETING ISO/IEC 27001 COMPLIANCE

Thierry Valdevit, Nicolas Mayer
CRP Henri Tudor, 29 avenue John F. Kennedy, L-1855 Luxembourg, Luxembourg
thierry.valdevit@tudor.lu, nicolas.mayer@tudor.lu

Keywords: information security, standard, compliance, SME

Abstract: Current trends indicate that information security is critical for today's enterprises. As managers realise they cannot ignore the potential security risks, they tend to turn to the ISO/IEC 27001 standard, in order to implement an Information Security Management System (ISMS). While being adopted by large companies, ISMS are still considered as out of range by numerous smaller entities. To help SMEs to access to ISO/IEC 27001 certification is still a challenge. In this context, the initial step of an ISMS implementation project is significant: a gap analysis highlighting the current status of the enterprise with regards to the standard, and thus the resources needed to succeed in this project. This paper presents the method and research works performed in order to design, experiment and improve a SME-oriented gap analysis tool for ISO/IEC 27001.

1 INTRODUCTION

It is now a well-known fact that information security is critical for enterprises and that a major impact can bring their activities to an end. In the past two years, 52% of businesses have experienced an unforeseen interruption, and the vast majority (81%) has caused the business to be closed for one or more days (Agility Recovery Solutions *et al.*, 2009). To tackle with this issue, the International Standardization Organization (ISO) published in 2005 the ISO/IEC 27001 standard, describing how to establish an Information Security Management System (ISMS). ISMS are now the common answer to manage the security of an information system in an organisation.

In order to implement this standard, most organisations start by evaluating the gap between their current status and the standard's requirements. This step is essential to estimate the resources required and to give an overview of what could be reused within the current system. Commonly referred to as gap analysis, this task is often complex. Indeed, the standard is composed of about 150 normative requirements for the ISMS and 133 security controls. Obviously, in the context of an SME, assessing each of these items is inefficient. Thus, it is a necessity to reduce the cost and complexity of this essential step.

The objective of this research work is to analyse the needs and conceive a tool to deal with this concern. Hence, the research question studied in this paper is: *how to quickly assess the compliance of an information system with the ISO/IEC 27001 standard?* Moreover, as our context is currently focused on SMEs, it is crucial to take into account their specificities such as limited maturity, resources and time. Our outcome is to define an efficient gap analysis tool providing a good overview of an organisation's status regarding the standard and its appendix.

In this paper we first present in Section 2 the ISO/IEC 27001 standard and its implementation process. Then, Section 3 describes the motivations for a tool related to gap analysis. The research method used to build this tool is outlined in Section 4. Next, the three steps of our research method are detailed respectively in Sections 5, 6 and 7. Finally, conclusions are given in Section 8.

2 THE ISO/IEC 27001 STANDARD

The outcome of ISO/IEC 27001 (ISO, 2005) is the effective establishment and management of an ISMS. The purpose is a continual improvement of information security. Relying upon quality

management 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.

The standard contains a set of normative requirements one must comply with to obtain the certification. The whole ISMS must be supported by specific requirements regarding documentation, management responsibility, internal audits, management review of the ISMS and system improvement. Moreover, the standard requires the selection of security measures among those listed in the informative *Appendix A*. It consists of a list of 133 security controls covering 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).

Next sections of this paper are dedicated to the development of a gap analysis assessment tool covering both the normative requirements and this appendix.

3 MOTIVATION AND INITIAL EXPERIMENT

Our initial experiment of ISO/IEC 27001 implementation was conducted from 2006 to 2008. The objective was to identify SME's strengths and weaknesses with regards to the standard. The project consisted in helping a national SME to establish an ISMS and succeeded in 2008 when it became the first private company ISO/IEC 27001 certified in Luxembourg (Valdevit *et al.*, 2009).

Through this initial experiment, we observed the importance and potential impacts in terms of efficiency to carry out a proper gap analysis. Although this is not a normative requirement, this step is strongly recommended in order to adequately plan the ISMS implementation. Such analysis shall include an identification of the different procedures or practices already existing within the organisation and related to ISO/IEC 27001 requirements. Also, it shall identify what is currently missing to be compliant with the standard. These elements are key information to evaluate what are the necessary financial and human resources to achieve the ISMS establishment.

After having performed a gap analysis during our initial experiment, some conclusions were drawn. Firstly, going through each of the standard requirements is not necessary: some of them are redundant in the standard and should be merged. For example, the requirements *4.2.1.a "Define the scope and boundaries of the ISMS…"* and *4.3.1.b "The ISMS documentation shall include: [...] b) the scope of the ISMS (see 4.2.1a)"* are both dealing with the same item.

Secondly, the various questions involve different roles and responsibilities among the SME, and therefore, different persons. These repeated changes of interlocutor and subject are inefficient. For example, the management involvement and commitment should be checked in a simple and unique flow, instead of assessing separately the different requirements related to this topic and spread across the standard (e.g., 4.2.1.b5, 4.2.1.h, 4.2.1.i, 5.1, A.6.1.1, etc.).

Finally, several requirements are too complex for people not aware of security and ISMS. For example, our initial experiment shows that the questions related to the different steps of risk management are not easy to understand for a non-specialist. Therefore, it is necessary to provide additional information clarifying the questions asked.

Ultimately, the gap analysis should be improved at three levels: remove redundancies, structure the assessment around thematic sections to increase fluency and reduce complexity.

4 RESEARCH METHOD

In order to reach our objectives in a structured way, we propose a research method inspired by action research approaches (Susman *et al.*, 1978) where theoretical work and practical experiments are cycling (Avison *et al.*, 1999) to iteratively enhance the results. In our context, the research method consists of three major steps:

Step 1 – *Modelling of the ISO/IEC 27001 requirements*: The structure of the standard does not fit the gap analysis needs. Thus, we propose to organise the standard through classes where each requirement has then to be classified. This step should simplify the structure of the standard by removing redundancies. It will also help to focus on the relevant actors for each part of the analysis. Completeness is a priority in this step. Each

requirement of the standard has to be considered and linked to a class. Therefore, an iterative cross-checking of the standard with regards to the model is necessary. The objective is to reach a relevant and homogeneous model, having a limited number of classes (between 10 and 15), each of them covering a limited number of requirements.

Step 2 – *Design of the assessment tool:* Once the structure is set, a questionnaire shall be accordingly. Pragmatically speaking, for a light tool dedicated to SMEs, it is not reasonable to have a question for each requirement. It is thus necessary to define a hierarchical questionnaire, composed of general questions, providing an overview of the topic assessed in each class. These general questions are completed with more precise ones, assessing each requirement of the standard, but used only if necessary. By rewriting and aggregating the questions, this step should produce a comprehensive and light questionnaire, later supported by a software tool.

Step 3 – *Experimentations*: Once a stable version of the tool is defined, the results shall be validated through experiments. Two experiments are planned. They shall bring feedbacks regarding the tool, and demonstrate its efficiency compared to the traditional approach performed during our initial experiment.

Once these three steps are performed sequentially, this process shall be performed again in an iterative and incremental manner in order to take advantage of the feedbacks gathered during experiments.

5 MODELLING OF THE ISO/IEC 27001 REQUIREMENTS

As stated previously, the first step of our research method aimed at the simplification of the structure of the standard. We first defined a set of coarse-grained categories related with the key topics of the standard (e.g., documentation management, resources management, etc.) that were elicited during our first experiment. Following a previous work (Valdevit *et al.*, 2009), we distributed all requirements over this set of pragmatic categories representing major activities of the ISMS. We proceeded through iterative analysis, refining our classification. For each requirement not fitting in any of our classes, we created a new one, or extended the scope of an existing one. After the last iteration, each requirement of the standard's core was linked to a suited category. The same process has been performed with the standard's appendix, mapping its 133 security measures in different categories.

The final task consisted in merging these 2 sets of requirements to delete redundancies between the core of the standard and its appendix. Indeed, some security controls of the appendix, like incident management or security awareness, are also mentioned as requirements within the core of the standard. As a result, 4 classes were merged, addressing security management, human resources management, monitoring and review.

In the end, the final set of classes (after the experimentation step depicted in Section 7) was reduced to 10 topics.

6 DESIGN OF THE ASSESSMENT TOOL

In order to satisfy the second step of our research method, most of our work consisted in the design of a pragmatic, clear and hierarchically organised questionnaire. The objective here was to assess the coverage level of an organisation for each topic with as few questions as possible.

As a result, there are only a couple of general questions for each class. Those open and global questions let the interlocutor answer freely. However, to ensure a complete coverage of each requirement, we implemented complementary sub-questions. Those closed questions shall be used only to assess a precise requirement, not covered by the answers to the open questions. They are thus rarely asked, but they serve as a support when additional information is required.

For each question, a 5-level rating is proposed, inspired by a standard on process assessment: ISO/IEC 15504 (ISO, 2003). These rating levels provide a progressive scale to assess the current practices within the organisation: N/A (requirement is intentionally ignored), not covered (no practice is done), partially covered (partially satisfied or in progress), largely covered (done but not sufficiently documented) or fully covered (satisfied and sufficiently documented).

In the end, the tool proposes about forty questions for assessing the coverage level of the 10 classes defined in Section 5. For a better comprehension and to ease the conclusions, the tool summarises the results of an assessment within two charts: a radar summarising the coverage of the

organisation's practices with regards to the requirements of the standard and a bar graph showing the respective requirements coverage of the *Plan*, *Do* and *Check* phases.

7 EXPERIMENTATIONS

The third step of the research method consisted in the experimentation of the tool in order to gather feedbacks and improvement opportunities. This took place as part of a larger experimentation field (Valdevit *et al.*, 2009). The tool was experimented in two different entities: the Luxembourg Airport Authority (LAA), a 150 people national administration, and IfOnline, a 4 people enterprise managing and maintaining a shared information system for several companies.

During those gap analyses, a specific attention was paid to class homogeneity, question understanding, time needed to perform the analysis and differences of results in assessments performed by several people at the same time. They made up our criteria for assessing the efficiency of the tool.

First experimentation at LAA was simple as this organisation has a certified quality management system. In the end, we identified 3 sections with abnormal duration compared to the others. Therefore we made changes in the structure of the model, merging two sections and moving a couple of questions.

The second experimentation took place at IfOnline. Its context was different as they have deep knowledge regarding security measures, but they were not experts on management systems. Due to the smaller size of the entity and the enhancements made to the tool after the first experiment, the analysis was 20% shorter. The different sections were homogeneous in terms of duration. Moreover, three analysts used the tool in parallel, and although the 5 qualitative rating levels of the questionnaire allow room for subjectivity, all three radar graphs (and thus the results) were close. After this experiment, a few additional minor improvements were made to simplify a couple of questions.

8 CONCLUSION

Following the growing interest about this standard, many SMEs aim at being ISO/IEC 27001 certified but lack the tools to start efficiently. The purpose of this paper is the development of a tool for quickly assessing the compliance of the information system of an SME with the ISO/IEC 27001 standard. To develop this tool, a research method composed of three steps has been defined. The first one is the modelling of the standard's requirements to develop a complete and simplified structure of thematic classes. The second step is the design of the assessment tool, based on a questionnaire. For each class of our model, a set of questions assesses the coverage level of an SME on a 5-level scale. Finally, the last step of the research method is the experimentation of the tool in two different SMEs.

As a conclusion, we can claim that our tool improves the efficiency of the gap analysis task. The results of the experiments show that the time needed to perform the gap analysis is reduced and that the questions are homogenously assessed by the analysts, based on the answers of the auditees.

Regarding future work, in order to improve validation, we first need to experiment our tool with external analysts, not involved in the development of this project. Furthermore, we would like to support the next tasks of the standard implementation, mainly by providing a modelling framework for risk management (Mayer, 2009).

REFERENCES

Agility Recovery Solutions, Hughes Marketing Group. 2009. Disaster Recovery & Business Continuity Survey.

Avison, D., Lau, F., Myers, M., Nielsen, P.A., 1999. Action Research. *Communications of the ACM*, Vol. 42, No. 1.

ISO, 2003. ISO/IEC 15504-2: Information technology – Process assessment – Part 2: Performing an assessment.

ISO, 2005. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements.

Mayer, N., 2009. Model-based Management of Information System Security Risk. PhD thesis, University of Namur.

Susman, G., Evered, R., 1978. An Assessment of the Scientific Merits of Action Research. *Administrative Science Quarterly*, Vol. 23, No. 4.

Valdevit, T., Mayer, N., Barafort, B., 2009. Tailoring ISO/IEC 27001 for SMEs: A guide to implement an Information Security Management System in small settings. In *Proceedings of the 16th European Systems & Software Process Improvement and Innovation Conference*, Springer Berlin Heidelberg.