
Thierry Valdevit, Nicolas Mayer, and Béatrix Barafort

CRP Henri Tudor, 29 avenue John F. Kennedy, L-1855 Luxembourg, Luxembourg
{thierry.valdevit,nicolas.mayer,beatrix.barafort}@tudor.lu

Abstract. While Information Security Management Systems (ISMS) are being adopted by the biggest IT companies, it remains quite difficult for smaller entities to implement and maintain all the requirements of ISO/IEC 27001. In order to increase information security in Luxembourg, the Public Research Centre Henri Tudor has been charged by the Luxembourg Ministry of Economy and Foreign Trade to find solutions to facilitate ISMS deployment for SMEs. After an initial experiment aiming at assisting a SME in getting the first national ISO/IEC 27001 certification for a private company, an implementation guide for deploying an ISMS, validated by local experts and experimented in SMEs, has been released and is presented in this paper.

Keywords: Information security, ISO/IEC 27001, SME, implementation guide.

1 Introduction

In 2008, financial frauds were displayed at the top of security incidents charts [1]. Nowadays viruses are becoming less alarming than notebook thefts. However, organisations tend to buy additional security products when security incidents occur. There is currently a strong need for a reliable and managed information security that does not focus only on technical solutions. Since 1995, the interest in risk management standards never ceased to grow. The British standards BS 7799 [2][3], which gave birth to both ISO/IEC 27001 [4] and ISO/IEC 27002 [5] ten years later, became more and more successful among organisations concerned by information security management.

Since their international development through ISO/IEC 27001, Information Security Management Systems (ISMS) [4] are known to be the systematic organisational answer to information security problems. They set the requirements for a global and self-improving environment to manage information security. In 2009, over 5000 organisations worldwide have already certified their ISMS [6].

To enhance the promotion of innovation and improve the overall maturity of organisations [7], Luxembourg's Ministry of Economy and Foreign Trade has charged the Public Research Centre Henri Tudor to establish a strong link between standardisation and end-users by spreading ISMS to SMEs (companies with less than 250 employees) in Luxembourg. As they represent 90% of the country’s organisations, it...
is legitimate to evaluate how easily could ISO/IEC 27001 be deployed across SMEs. This research work lies on the expertise that has been developed for several years in CRP Henri Tudor in Information Security [8], assessment and improvement of processes using the ISO/IEC 15504 standard (Process assessment) in several sectors and disciplines [9][10][11], downsizing standards for SMEs and transferring competences to the market via the development of labels and/or certifications [12].

The particular underlying research project developing the ISMS implementation guide for SMEs aims at helping them to go towards the implementation of a simpler ISMS. The focus of this paper is thus based on the following research questions:

1. What are the specific needs of SMEs regarding ISMS?
2. How can we adapt ISO/IEC 27001 to best suit SMEs?

The paper is structured as follows: Section 2 presents the ISO/IEC 27001 standard. Then, Section 3 presents our research method. Section 4 discusses the initial experiment that triggered the definition of our particular objectives for an ISMS implementation guide adapted to SMEs. Section 5 reports the various steps of the elaboration of the guide. Section 6 presents the future work required by the project. Finally, Section 7 concludes this paper and opens discussions regarding the research method and the strengths and weaknesses of the results.

2 The ISO/IEC 27001 Standard

The outcome of an ISO/IEC 27001 certification is the effective establishment and management of an ISMS. Relying upon quality management and ISO 9001 [13] principles, it is built around a PDCA (Plan-Do-Check-Act) cycle, which objective is a continual improvement of information security.

For an organisation to be certified, it is necessary to be compliant with the set of normative requirements defined in the ISO/IEC 27001 standard. Those requirements are expressed from Section 4 to Section 8 of the standard [4]. The other sections are considered to be informative, and thus are not mandatory for the certification. The set of normative requirements can be summarised as represented in Figure 1. This figure presents the different parts of the standard, structured by sections.

First of all, 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). These steps are supported by a specific documentation, whose requirements are explained in Section 4.3. Along with the documentation, they represent the core requirements that one should satisfy to be certified. Additionally, some requirements are especially developed in a dedicated section, because of their importance or complexity. The first one in this case is the management responsibility, describing where it is necessary for the management to be specifically involved (Section 5). A part is dedicated to the way to perform the internal ISMS audits, which are mandatory (Section 6). Regular management reviews are also necessary in the cycle (Section 7). Finally, the normative requirements sections end with requirements on how to perform the ISMS improvement (Section 8).