Codasystem first to obtain ISO/IEC 27001

Nicolas Mayer
Sébastien Pineau

Certification has become a key trust factor between organisations. The ISO 9001 standard for quality, or the ISO 14001 one for environment, are concrete examples showing that management systems and associated certification are now widely spread on the market.

The ISO/IEC 27001 standard, published in 2005, deals with information security management. Information security is currently a core concern for organisations. Aware of these needs and competitive matters, CRP Henri Tudor is stressing works on R&D products and services development, based on security standards and certification frameworks.

Despite its importance, the current state is that very few organisations are currently certified for their Information Security Management System (ISMS) in Luxembourg. Up to now, the only one in Luxembourg was the "Loterie Nationale". The ISO/IEC 27001 certification is considered as complex and difficult to set up, mainly for SMEs, having generally a low budget and very few human resources to allocate on such a project. Thus, CRP Henri Tudor has developed methodological tools and services to assist companies during their certification process. A Luxembourg SME named Codasystem committed itself to experiment tools and methods developed by CRP Henri Tudor, for supporting SMEs in their certification process.

CRPHT's R&D activities' benefits

The experimentation started in June 2006 and ended in May 2008. It consisted in establishing and managing an ISMS. The ISMS is built on a continuous improvement of security, allowed by following a Plan-Do-Check-Act methodology. The objective of this collaboration was to have a 'win-win' approach. CRP Henri Tudor brought its methodological tools and knowledge of the ISO/IEC 27001 standard, and transferred it to Codasystem. For its part, Codasystem provided a feedback on the tools and helped to review and improve the research products and services.

One of the core parts of the experimentation was about techniques for performing risk assessment. It starts with the identification of key assets of the company. Then, risks harming these assets are identified. We thus define potential threats, exploiting security vulnerabilities and leading to impacts to the assets. All of these components are estimated, in the aim of defining the risk levels, and, further, which of them are inacceptable, with regards to the business objectives. Finally, inacceptable risks are treated with adapted solutions, generally through the definition of security requirements.

Solid method

A solid method was proposed for tackling all the previous points. This method includes a process, describing the different steps to satisfy the standard requirements related to risk assessment. Moreover, learning artefacts are also included, in the aim of facilitating the method understanding by the risk assessment team, but also to enhance security awareness for the whole company. Identification of assets was done through process modeling. Then, risk identification and estimation was performed by combining techniques and knowledge bases of existing risk management methods, with methodological tools adapted by CRP Henri Tudor to the SME context. This experimentation has been completed some months ago and the project fully achieved its objectives: Codasystem became the first private company of Luxembourg being ISO/IEC 27001 certified.

Developing products

The CRP Henri Tudor aims at going further in this way and continues to develop products and services to assist companies, mainly SMEs, to implement an ISMS and meet the ISO/IEC 27001 requirements. The current R&D topic is the definition of an implementation guide, aiming at satisfying part of the entire set of requirements. This guide naturally lies on the feedback provided by Codasystem during the first experimentation. The objective of this guide is not to completely prepare a company to be ISO/IEC 27001 compliant, but to prepare the ground for implementing an ISMS.

In accordance with the objectives of the "Ministère de l'Economie et du Commerce extérieur", the guide only assists the company with starting taking care of information security, by getting over a first step towards the complete implementation of an ISMS. A sub-part of the standard requirements has indeed been selected in the guide, in order to decrease its complexity. This guide is currently in a validation process, supervised by Luxembourg experts. Once this theoretical validation is performed, a practical one will start, by experimenting the guide within SMEs.

The authors are from the CRPHT Nicolas Mayer:
nicolas.mayer@tudor.lu
Sébastien Pineau:
sebastien.pineau@tudor.lu