Tailoring ISO/IEC 27001 for SMEs: A guide to implement an Information Security Management System in small settings

Thierry Valdevit[1], Nicolas Mayer[1], Béatrix Barafort[1]

[1]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).

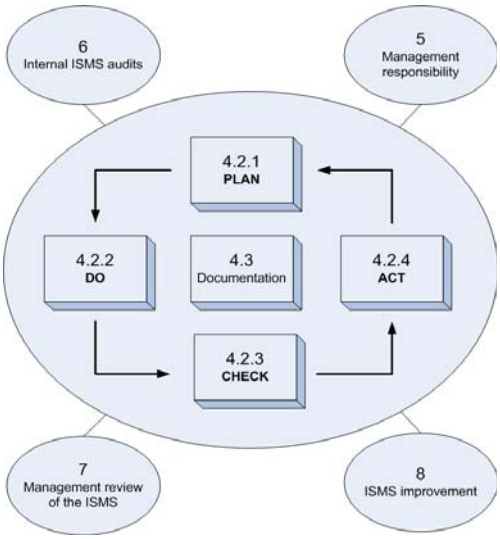

Fig. 1. The ISO/IEC 27001 group of requirements

3 Research Method

In order to answer our research questions in a structured way, we propose a research method following an action research approach [14]. It can be defined as "an iterative process involving researchers and practitioners acting together on a particular cycle of activities, including problem diagnosis, action intervention and reflective learning" [15]. The research method, presented in Figure 2, consists of three steps.

Step 1 – *Initial experiment*: An initial experiment is performed in a Luxembourger SME. In order to identify the issues related to the implementation of an ISMS in such an entity, many feedbacks are gathered from this experiment. Then, they are summarised to put emphasis on the major issues encountered. Hence, our research objectives are defined so as to address those issues. This step answers our first research question.

Step 2 – *Building the guide*: The guide is written in order to achieve the objectives identified during the first step of the research method. To ensure the relevance and the viability of the document, it is validated through experts' reviews. To do so, Luxembourger experts in information security are mandated to theoretically evaluate the guide. This process, closely tied with field experiments (Step 3), gives feedbacks in order to improve the guide.

Step 3 – *Experimenting the guide*: As theoretical validation cannot bring an insurance of effectiveness and adaptability of the guide, experiments are required within the research method. They take place in several SMEs with different security backgrounds and from different activity sectors. These experiments are not only conducted by our team, but also by external individuals, in order to assess the usability of the guide by people not involved in its development process. Each experiment leads to several feedbacks and initiates upgrades to the guide.

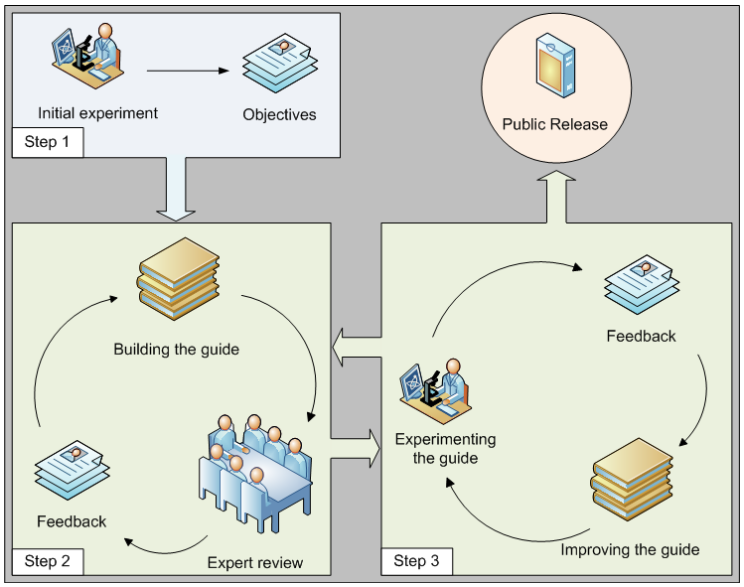

Fig. 2. Research method

Step 2 and 3 are performed iteratively, with consecutive updates of the guide. After each reviewing process, a concrete experiment is planned bringing feedbacks and updates to the guide. These modifications are then validated or modified through another expert review and a new experiment can be started. After several iterations, the guide should be freely available to SMEs.

4 Initial experiment

The initial experiment was conducted in a SME in Luxembourg called Codasystem [16]. This company offers innovative security services based on new information technologies. The value proposition associated to their services is based on the management of the authenticity of digital documents. The Codasystem product addresses the need for a reliable, secure and easy to use system capable of circumventing falsification risks both on electronic documents and exchanges. Currently, solutions available on the market are focused on securing exchanges (authentication, email signatures, cryptography). No solution exists that could provide indisputable proof in court for both the electronic document and its exchange. Codasystem offers the first integrated solution for the creation of digital proofs and their secure distribution (see Figure 3). The solution of Codasystem has been examined by a law firm expert in digitalisation and legal property, and has received approval regarding its legal value. The technology of Codasystem is patented in France and extended worldwide.

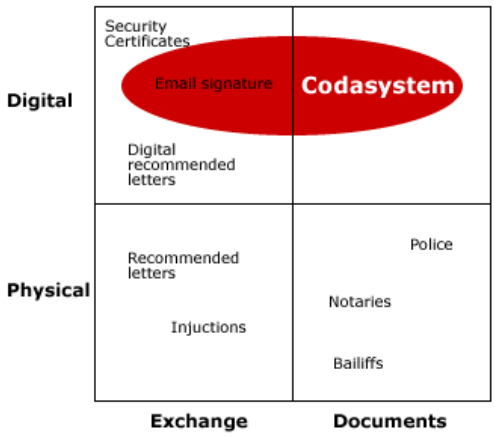

Fig. 3. Proposed product of Codasystem

Although the product proposed by Codasystem has been approved by experts, the security of their processes is also at the heart of their concern. That is why the improvements in terms of security and the trust granted by the ISO/IEC 27001 certification were raising strong interests.

4.1 Implementation of Codasystem's ISMS

The initial experiment (Figure 2) at Codasystem started in June 2006 and ended in May 2008. The collaboration between our team and Codasystem is evaluated at about 100 CRP Henri Tudor man-days. The total documentation produced was over 300 pages.

The complete process was very long and time-consuming. This is actually due to several issues. First, the set of ISO/IEC 27001 requirements to satisfy is very important, especially for a SME like Codasystem with few human resources to allocate on this project. Moreover, the gap between the current state of an SME and the state to reach for the certification is generally more important in SMEs. For example, a resource management process is typically in place in large organisations, as opposed to SMEs where it is usual to develop it "from scratch". Very few formalised policies or procedures were already available in Codasystem.

The average knowledge of people involved in the setting up of the ISMS is also generally lower in a SME than in a large company. Where large companies are able to hire experienced and skilled human resources with regards to management systems, SMEs generally choose internal employees who include their effort on the ISMS in their day-to-day work. That was the case within Codasystem, where people had not much knowledge in quality and process management. Many training sessions were performed during the early meetings of the experiment, in order to familiarise the team with the standard.

The time needed to develop the documentation and to satisfy all the requirements was also very important. Hopefully, our knowledge was an added value to the

Codasystem's team, because they had very few experiences on what to implement in order to satisfy the requirements.

After nearly two years of experimentation, Codasystem became the first private company ISO/IEC 27001 certified in Luxembourg, thus successfully concluding the first step of our project. Moreover, all the lessons learnt during this experiment have provided significant inputs for Step 2 of the project. They are summarised in the next section.

4.2 Identification of the objectives of the guide

As seen in the previous section of the paper, this first experiment with Codasystem brought us interesting feedback regarding the implementation of an ISMS in a SME. Those inputs have been analysed in order to highlight some key issues and thus have shown the challenges of such a research project. As a result, a methodological guidance is indeed necessary, in order to achieve the following objectives:

- Objective 1: *Downsize the requirements in order to reduce the cost and the complexity of an ISMS*. The set of ISO/IEC 27001 requirements has to be scaled down, in order to fit with the limited resources of most SMEs.
- Objective 2: *Smooth the approach to the users*. Implementing an ISMS should not be perceived as a constraint imposed by business strategy. Therefore, a smooth approach has to be developed introducing processes, PDCA paradigm and management systems benefits to users.
- Objective 3: *Give the major recommendations and generic tasks to ensure the proper operation of the ISMS*. Part of the work is transversal, like documentation management and management responsibility: it takes place all along the successive PDCA tasks. Therefore, the guide should start by presenting these specific actions, detailing how they affect the whole system.
- Objective 4: *Provide implementation guidance for each process of the PDCA cycle*. ISO/IEC 27001 presents all those requirements in a rough listing while the presentation of these items should require a simple, standard and clear pattern. All the inputs needed to ease fulfilment should also be provided.
- Objective 5: *Ensure coherence and reliability of this tailored handbook*. The goal is to allow the possibility of having a smooth transition towards ISO/IEC 27001 certification. Therefore, the guide has to remain strictly aligned with the original requirements, in order to necessitate only simple improvements if a SME wants to achieve a certification.
- Objective 6: *Provide tool support*. A framework of documentation tools and templates should be proposed as a support for the implementation. The aim is to accelerate the process of implementation and decrease the cost involved (particularly for documentation). It should also serve as a basis for packaged market-oriented solutions and services (next transfer part of the research project).

5 Building the guide

In order to achieve the objectives set in Section 4.2 of this paper, the guide has been built with these specific aspects in mind. The following paragraphs explain how we tackle the issues highlighted in the preceding ones.

5.1 Selective coverage

As an answer to the first objective, we propose in the guide a tailored version of the ISO/IEC 27001 requirements. The complete set of standard requirements was first modelled as a list of 32 major activities. Each of them was annotated, if applicable, with its key outputs in term of document production. This list was then split over a 5-column matrix representing various progressive configurations, giving five coherent set of activities. Those five choices have been established through multiple experts' opinions in order to find a consensus that would maintain coherence for each column and keep the smoothest progression from implementing level 1 to 5.

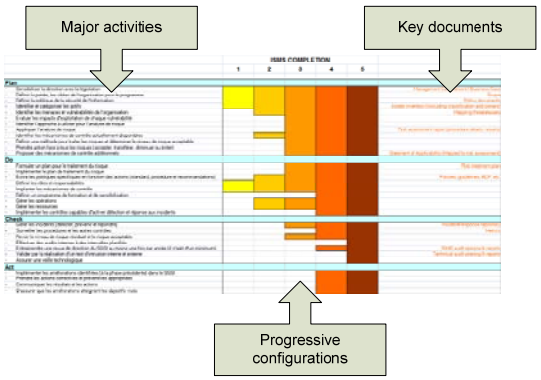

Fig. 4. ISMS completion matrix

The criteria used to define these configurations were essentially in connection with resources consumption, importance of the activity within the ISMS and therefore return on security investment. However, the impact of each choice was taken into account for its relevance with regards to the whole ISMS's efficiency. Indeed, numerous activities are strongly tied together and cannot be removed nor added without others. For instance, the risk assessment requires half a dozen of activities, which have no meaning by themselves.

Finally, a given level was chosen: implementation level 4. It basically consists of a complete ISMS, without audits requirements, nor technical surveys. On one hand, level 3 was rejected as it lacked most "check/act" activities. On the other hand, level 5 was too close to the original standard to bring any added value to the guide. Furthermore, as audits were probably one of the most expensive and time-consuming part in Codasystem's experiment, it made sense to remove them.

Decisions made with this matrix conducted to the definition of the ISO/IEC 27001 coverage of the guide. This modelling of the standard also served as guidelines regarding how the guide should be organised, as explained in Section 5.4.

5.2 Raising awareness and maturity to lower apprehension

As stated in Objective 2, initial apprehension can be critical regarding ISMS implementation. That is to say, if the management perceives an ISMS as a long, costly or useless approach, it will not fund its implementation. Therefore, the guide starts with some introduction chapters, which aim at answering most common doubts and misconceptions, and motivate the use of the guide.

First, 10 key concepts are explained such as “asset” or “residual risk”. This introduction page covers the most important concepts used all along the document into a convenient condensed form. It gives the prerequisites to understand the guide and keep it self-sufficient. Then, the reader is introduced to ISMS, by providing more information on their goals and reducing common misconceptions regarding information security. In order to highlight the scope of the guide, the gap with the actual ISO/IEC 27001 is detailed and explained. Subsequently, quality management and process approaches are presented by giving the necessary knowledge to understand the PDCA paradigm.

In the end, raising awareness is tackled with some advices about the state of mind and maturity required before implementing an ISMS. A whole chapter dedicated to the estimated implementation period supports this last part. A generic distribution of each stage is given as an example of how PDCA iterations should be conducted.

5.3 Transversal guidelines

ISMS deployment does not only rely on the successive tasks recurring within the PDCA cycle. Indeed, the standard contains requirements supporting the whole PDCA chapters, as mentioned in Objective 3. Four chapters focus on those specific concerns and serve as the very first steps of the implementation, prior to the beginning of the “Plan” stage.

First, the guide insists on the importance of obtaining a written management commitment regarding the requirements and consequences of ISMS. Indeed, the management often takes lightly all the implications of such a project in the company. By asking for this document, the guide ensures that management has considered those aspects.

Second, it gives all the required information on how to manage documentation within the system. Focus is made on the importance of having a proper documentation policy and generic guidelines are given to classify each document regarding its origin, access restriction, storage and disposal.

Third, users are invited to build a document referencing and assigning human resources. The guide proposes four generic categories of actors involved in the various tasks of an ISMS. Assigning people on those roles eases the implementation because each step is linked to those categories.

As a conclusion to transversal guidelines, the guide insists on deontological ethics all along the life cycle of the management system.

5.4 Key steps presentation

The standard is not user-friendly enough to be handled by most SMEs (Objective 4). Consequently, in order to facilitate the readability and comprehension of the guide, each process is presented using a simple pattern inspired by Process Reference Models (PRM) [17].

B. Implement anomaly management process

Details	The efficiency of the ISMS is insured by detection mechanisms, monitoring, records and anomaly correction.
Tasks	Define and apply anomaly management process including the following items: 1. Identify the anomaly (incident, non conformity, etc.) 2. Diagnostic method 3. Creation of anomaly ticket (synthetic record containing useful information regarding the anomaly) 4. Possible escalation 5. Anomaly resolution procedure 6. Anomaly enclosing
Inputs	Enterprise's organisation
Outputs	Anomaly management process Anomaly tickets
Actors	Every level of management ISMS accountable Employees

Fig. 5. Process description example

For each process selected in the guide (see Section 5.1), the guide presents:

- Its name

Most processes are named like their ISO/IEC 27001 equivalent, but little adjustments were made to obtain more generic and global terms, which represents more clearly their content.

- Its description

In order to facilitate comprehension and enhance efficiency, the guide includes awareness-raising elements all along its content. It explains for each process its motivations, utility and consequences.

- The detailed tasks

Processes are split across a simple set of tasks containing the sub-actions that should be completed. They are first aggregated according to Codasystem's feedbacks for readability and understanding, and will be improved after the next experiments.

- Input/output documents and records

Linking the various steps to each other is complex. Thus, to facilitate organisation of documents and “out of the box” deployment, each process directly refers to its inputs and lists its own outputs. In this way, it is easier to mesh all the processes together and facilitate templates production and use.

- The people involved

As stated previously (Section 5.3), four categories of actors are defined. Those key roles are assigned to each process when needed, giving immediate information regarding who should be involved and what are the hierarchical implications.

5.5 Experts validation

ANSIL is the Luxembourg Information Society Standardisation Association. This national association contributes to IT standardisation activities in Luxembourg, from the creation of experts committees to the promotion of standardisation. Within this association lies the CNLSI (Information Security Standardisation Committee: mirror group of ISO/IEC JTC1 SC27 in Luxembourg) which is composed of a dozen of experts in information security. They were mandated to review and comment the guide (theoretical review) twice, thus ensuring the achievement of Objective 5.

On the first validation cycle, in November 2008, they conducted 3 iterative reviews in the same way as ISO standards are reviewed. Overall, they issued 156 comments requiring various modifications of the guide. Prior to the first experimentation stages, this initial validation ensured the document's reliability, coherence and alignment with ISO/IEC 27001.

The second reviewing process is planned to take place after the first SME experiment (see Figure 2). It will expectantly give new feedbacks, thus ensuring the quality of the final version of the guide.

5.6 Tool support

In agreement with Objective 6, a methodological guidance does not help enough the users in order to implement an ISMS. To cope with this issue, we have developed numerous templates and documentation tools mostly based on Codasystem’s experiment. They ease and speed up the implementation of the ISMS, enabling users to focus on more complex tasks, thus reducing the amount of human resources required.

Regarding documentation, we created numerous generic procedures to be completed and tailored by end-users. Our templates (i.e. management commitment, ISMS policy, anomaly management procedure, etc.) only require to fill a few blanks, and sometimes to be slightly adapted to the context of the organisation, before being used.

For the most complex part of the ‘Plan’ phase, that is to say risk assessment, a specific tool has been developed following an innovative model for risk management [18]. It assists the user all along the risk assessment steps and is compliant with ISO/IEC 27005 [19].

6 Further experiments and upgrades

Experimental results in Codasystem showed numerous opportunities to improve and scale down an ISMS to fit to SMEs' needs. That is why the project's method integrates two experimentation stages.

After 6 months of development and reviews, the guide is currently assessed in a public (SME-sized) administration. Later on, a complete experimentation panel will take place by supervising the deployment of the guide among three candidate SMEs from various sizes and businesses. This second experimentation stage will be conducted in a mutualised and interactive manner. Indeed, the ISMS implementation of the three SME’s will be synchronised. Collective training sessions will be performed and completed with individual on-site coaching. During combined courses, the three SMEs will discuss their progress together, bringing new ideas and more feedbacks to improve the guide even further.

7 Discussion and conclusion

In this paper, we have first analysed what are the specific needs of SMEs regarding ISMS. Then, we have proposed a research method in order to tailor the ISO/IEC 27001 standard to an adapted way for SMEs. The two first steps of this research method have been already performed and the third step is currently in progress. Furthermore, the theoretical validation, that is part of the second step, will be performed again, in order to improve the guide iteratively after experiments. The outcome of this research work is a guide providing a more affordable, easier and faster way to implement an ISMS that is still covering a vast majority of ISO/IEC 27001 requirements. This way, this research project brings combined benefits for the Luxembourger market: it promotes information security to SMEs through the guide, and it provides local IT consultants with a wider range of methodological support.

Regarding strengths of our approach, the systematic research method proposed in Section 3 blends theoretical reviews and experiments. Furthermore, the experiments are not only conducted by our teams, but also by individuals apprehending the guide for the first time. We thus ensure objective feedbacks about our research work.

Moreover, this guide looks convenient on many aspects. Indeed, by approaching management systems from the very beginning and dispensing the required knowledge to understand why and how ISMS should be deployed, the guide gets a strong head start when compared to the raw ISO/IEC 27001 document. The presentation pattern listing both human and documentary resources eases the understanding and speeds up the deployment of an ISMS. Combined with the limited coverage of the standard, the guide grants the possibility to easily focus on the core elements of an ISMS implementation and therefore increases overall efficiency.

However, each action to make the guide simpler is one step away from the initial standard. Certainly, the reduced scope causes potential troubles. Audits are definitely a good mean of detecting problems within one's organisation and helps setting milestones regarding ISMS status.

Finally, individuals could wonder why they should implement such a guide instead of targeting a direct ISO/IEC 27001 certificate. Given this statement, the guide should be part of a complete labelling framework for SMEs, supported by the Ministry of Economy and Foreign Trade, and potentially a national certification dedicated to SMEs. The development of this framework is part of our future work.

8 References

1. CSI, 2008 CSI Computer Crime and Security Survey (2009)
2. BSI, BS7799-1: Information Security Management Systems – Code of Practice for Information Security Management Systems (1995)
3. BSI, BS7799-2: Information Security Management Systems – Specification with guidance for use (1999)
4. ISO, ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements (2005)
5. ISO, ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management (2005)
6. ISO, Information security management systems for small and medium-sized enterprises. ISO Management Systems, Vol. 9, No. 1 (2009)
7. Information Security Portal in Luxembourg (2009), `http://www.cases.public.lu`
8. Barafort, B., Humbert, J-P., Poggi, S.: Information Security Management and ISO/IEC 15504: the link opportunity between Security and Quality. SPICE'2006, Luxembourg (2006)
9. Hilbert, R., Renault, A.: Assessing IT Service Management Processes with AIDA – Experience Feedback. EuroSPI'2007, Potsdam, Germany (2007)
10. Di Renzo, B., Valoggia, P.: Assessment and Improvement of Firm's Knowledge Management Capabilities by using a KM Process Assessment compliant to ISO/IEC 15504. A Case Study. SPICE'2007, Seoul, South Korea (2007)
11. Di Renzo, B., Hillairet, M., Picard, M., Rifaut, A., Bernard, C., Hagen, D., Maar, P., Reinard, D.: Operational Risk Management in Financial Institutions: Process Assessment in Concordance with Basel II. SPICE'2005, Klagenfurt, Austria (2005)
12. Renault, S., Dubois, E., Barafort, B., Krystkowiak, M.: Improving SME trust into IT consultancy: a network of certified consultants case study. EuroSPI'2007, Postdam, Germany (2007)
13. ISO, ISO 9001: Quality Management Systems – Requirements (2000)
14. Susman, G., Evered, R.: An Assessment of the Scientific Merits of Action Research. Administrative Science Quarterly, Vol. 23, No. 4 (1978)
15. Avison, D., Lau, F., Myers, M., Nielsen, P.A.: Action Research. Communications of the ACM, Vol. 42, No. 1 (1999)
16. Codasystem (2009), `http://www.codasystem.com`
17. ISO, ISO/IEC 15504-2: Information technology – Process assessment – Part 2: Performing an assessment (2003)
18. Mayer, N.: Model-based Management of Information System Security Risk. PhD thesis, University of Namur, Belgium (2009)
19. ISO, ISO/IEC 27005: Information technology – Security techniques – Information security risk management (2008)