Information Security Management and ISO/IEC 15504: the link opportunity between Security and Quality.

Béatrix Barafort
Jean-Philippe Humbert
Sébastien Poggi
Centre de Recherche Public Henri Tudor
Centre d'Innovation par les Technologies de l'Information
29, avenue John F. Kennedy
L-1855 Luxembourg
beatrix.barafort@tudor.lu
jean-philippe.humbert@tudor.lu
sebastien.poggi@tudor.lu

Abstract

Information and Communication Technology (ICT) development transformed our worldview by bringing closer everyone and everything at the electron's speed. This mutation represents a tremendous step and enabler for knowledge, human relations and economy. Consequently, information became a more strategical and valuable resource than ever as the development of such field like economics intelligence underlines it; and like the others, this resource must be protected. Information Systems Security (ISS) deals with this issue with theoretical tools, base practices and standards. However, the remaining question is: "How to bring these tools into organizations and everyday work?" By using quality tools such as ISO/IEC 15504 standards in conjunction with the latest advancement in information security management, a process reference model and a process implementation model have been developed to provide a framework for assessing and increasing process capability and organizational maturity in the field of ISS. This concept presents multiple applications like defining a security policy based on processes, but also towards legal aspects, standardization, training, benchmarking, and, of course, assessment and certification.

1. Introduction

In the context of information systems dependant-companies, problems of confidentiality, availability, and integrity represent a huge challenge as the unceasingly complexity growing of technologies (Internet particularly) and their intrinsic vulnerabilities dependent on internal, or external threats, are exploding. Within this framework of issues, the Ministry of Economy and Foreign Trade of Luxembourg (MECOFT) takes part in the european Cyberworld Awareness and Security Enhancement Structure [1] (CASES), whose goal is to share useful information for preventing and protecting information and communication systems. In order to support the development of this structure, the MECOFT and the Public Research Centre Henri Tudor in Luxembourg [2] (CRP Henri Tudor) set up the R2SIC [3] project (Recherche pour la Sécurité des Systèmes d'Information et de Communication) to analyze and to exploit the information collected by CASES. These research tasks target on the one hand to fine tune the CASES actions through the project deliverables, and, on the other hand, the design of reference guides on the information security management in SMEs and for citizens, with the real cases addressed by the CASES network.

Four lines, detailed below, compound the R2SIC project. The first line performs research on the social actors responsibilities for the threats related to hacking, through the achievement of a PhD thesis in computer science[4]. The second one investigates on SME's security vulnerabilities. It collects information for a better understanding of the SME's current situation in Luxembourg in the field of ISS, and particularly on the tools impact for awareness and training about vulnerability management. The third line deals with the development of a reference framework suitable for SME's in Luxembourg. It contributes to the management of security in the light of the results of the second line, in a downsizing approach of the standards currently referring on the matter. The last one aims the multiplication of the CASES structure awareness and training means. It is based on an e-learning content development for citizens, in a "training for the trainers" view. It aims at optimizing the operational consequences of the two first lines.

Before this recent collaborative security research project, the cooperation between the MECOFT and the CRP Henri Tudor enabled to perform surveys for a national public key infrastructure scheme, a major contribution to the "National Information Security Network & System Plan", and a great participation in the development of CASES. In addition, the CRP Henri Tudor has developed a so-called information security innovation platform with partners and institutional stakeholders. This platform is a link between research projects, the CRP Henri Tudor strategy and the industry on that topic. Furthermore, in quality research domain, different thoughts and experiences with the ISO/IEC 15504 standard led the CRP Henri Tudor to the definition of several R&D projects in this scope [5][6], aiming at using multiple standards in a combined way. The standard for process assessment ISO/IEC 15504, resulting from the Software Process Improvement and Capability dEtermination (SPICE) major international initiative also plays an important role in this field.

The key idea behind the ISO/IEC 15504 [7][8][9][10][11] model enables organizations to assess themselves against a range of best practices in order to improve their processes or to determine suppliers' capability for these assessed processes and select the supplier that demonstrates the best capability. The main topic that interests us is the use of ISO/IEC 15504 standard in the sole context of process assessment and process improvement since its last evolutions allow to cover all activity sectors and not only the software one. In partnership within the R2SIC project, the CRP Henri Tudor and the MECOFT joined their security and ISO/IEC 15504 approach and expertise in order to model processes according to ISO/IEC 15504 requirements for Process Reference Model (PRM) and Process Assessment Model (PAM).

2. Information Security overview

2.1. Risks

Concerned by important risks, the information society must protect, in relation, any information system containing important assets. In order to manage these information system risks, ISS brings theoretical, methodological and practical tools. One of them, the risk equation, can be explained simply by the following formula [12]:

$$R \text{ (Risk)} = V \text{ (Vulnerability)} * M \text{ (Menace)} * I \text{ (Impact)}$$

which implies important theoretical concepts. Therefore, risk is resumed in a combination of vulnerability, threat and impact. Vulnerability is a security lack which can potentially be exploited by a threat. It can be technological (lack of use of antivirus and anti-Trojans software) or organizational (lack of correct and up-to-date password management in the company) applied to the information system. Consequently, a threat consists in an exploit relying on a vulnerability that can be divided into two categories:

- Passive if it does not modify the system behavior, or if it is undetectable (i.e. Trojans, spying programs invisible to the victim),
- Active if there is modification of the information contents (i.e. "defacement", transformation of a web site's home page).

The impact represents a prejudicial consequence to the organization that was the victim of the vulnerability exploitation by the threat.

2.2. Is it important to conduct a risk analysis?

Generally an organization conducts an "intellectual" and informal risk analysis meeting indeed business requirements. To lead a formal risk analysis, some products have been developed to facilitate this job for all kinds of organizations. A large choice is available; the difference relies on maturity and success for these methodologies. We can mention, for example, EBIOS [13] and OCTAVE [14].

When facing identified risks, the information security posture corresponds to the state of protection that results from the general and particular measures taken, formally or not, to ensure in particular the following security requirements: Confidentiality, Integrity and Availability (CIA).

- Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes [15]
- Integrity is the property of safeguarding the accuracy and completeness [16]
- Availability is the property of being accessible and usable upon demand by an authorized entity [15]

To ensure quality of the security scheme implemented and applied in an organization, a document summarizes all these requirements, the “security policy”. A security policy is an internal settlement that specifies how to manage, to protect critical assets, and to diffuse information. Many models exist to write a security policy but they do not address the target or the business concerned. Among these models an original concept has been also developed by the MECOFT, which proposes a security policy template for SMEs, specially downsized from the ISO 17799 standard [17], a collection of good practices to heighten the security level.

2.3. Existing standards

In ISS, a set of standards and methods are used to be the very reference for specialists. Among them, several kinds of documents can be identified [18] that are valuable resources for people dealing with ISS.

- ♦ Risk analysis-oriented
  EBIOS, OCTAVE, MEHARI, MARION
- ♦ Best practices oriented
  ISO 17799/BS7799-1, ITBPM, RFC 2196, ITIL
- ♦ Product oriented
  ISO 15408/Common Criteria, ITSEC
- ♦ Guidelines
  ISO 13335, NIST 800-30, PSSI, TDBSSI
- ♦ Process oriented
  ISO 21827/SSE-CMM, CobIT
- ♦ Several of the above
  CRAMM

A chain of actions is also implicitly defined in ISS to set up a security program. This “classic” chain of action is illustrated in Figure 1. From this point of view, security is a one shot approach.

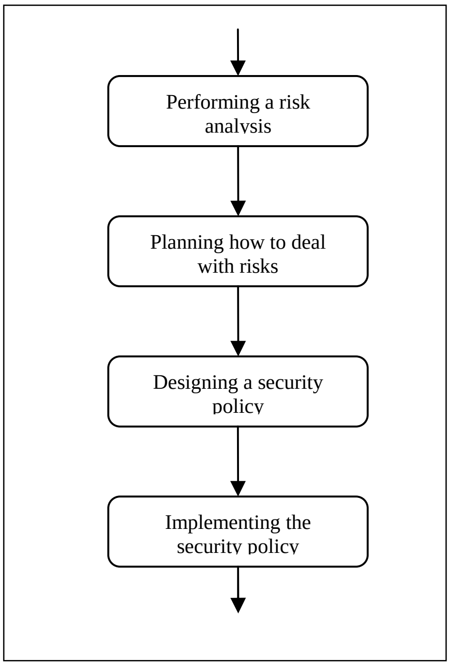

Performing a risk analysis
Planning how to deal with risks
Designing a security policy
Implementing the security policy

Figure 1. "Classic" chain of actions in an ISS project

The high-costing profile of ISS is another characteristic to consider in the aftermath because ISS requires a specific knowledge and high skilled individuals. Therefore, security products and services are very costly and require heavy investments for organizations. Chief Information Security Officers (CISO) with limited resources need metrics on efficiency about the implemented safeguards. Thanks to these metrics, they are able to make thoughtful decisions on how to optimize a security program. A Plan–Do-Check-Act [19] cycle is set up.

This PDCA approach mapped in ISS was actually promoted in the 2002 edition of the BS 7799-2 standard [20]. The BS7799-2 was released by the British Standard Institute to specify the requirements for implementing an Information Security Management System (ISMS), a concept that can be compared to the Quality Management System (QMS) introduced by the ISO 9001 [21] and the Environment Management System (EMS) proposed by the ISO 14001 [22]. ISS programs became continuously improving approaches. (Figure 2)

This point of view has been very recently approved by the ISO through the publication in October 2005 of the ISO 27001 standard [23], a transposition of the BS 7799-2:2002 that represents *de facto* the latest advancement in ISS organizations.

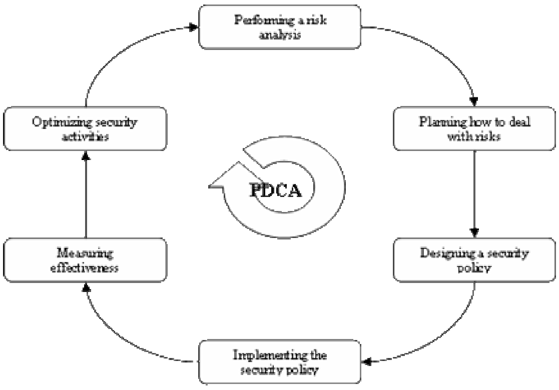

Performing a risk analysis
Planning how to deal with risks
Designing a security policy
Implementing the security policy
Measuring effectiveness
Optimizing security activities
PDCA

Figure 2. The "PDCA" chain of actions

3. Bridging the gap between security and quality

3.1. Using processes and ISO 15504 in the Information Security field

The newly created ISO 27001 promotes the use of processes. However, it does not formally specify what a process is or how a process has to be assessed. Actually, the process definition given by the ISO 15504 is extremely applicable to this field and provides a suitable scope for using processes to implement an ISMS, thus an opportunity for CISOs to introduce quality criteria in security. This is achievable through the structural strength of the standard.

Depending on its size, business, competition and lots of other factors, each organization has its own needs in terms of security requirements. To create an efficient and well-sized management system for the organization, the CISO or other security-concerned people can select the most relevant processes into a Process Reference Model (PRM). With the help of a Process Assessment Model (PAM) based on this PRM and the ISO/IEC 15504 Mesaurement Framework, the organization owns then all tools to optimize its security activities.

The process-oriented view especially suits ISS due to its transversal scope, as many business activities rely on ICT. Moreover, as zero risk does not exist, CISOs have not an obligation of results, (product oriented view) but of means (process oriented view) towards legal aspects and top management.

3.2. About the design of an ISMS PRM and an ISMS Process Implementation Model (PIM)

The main purpose of the ISMS PRM and PIM is to provide methodological tools for security-concerned people to assess and improve their security processes. To reach this goal, a complete set of major activities in this field has been identified, based both on a preliminary holistic study on security and quality standards (cf. 2.3. Existing standards) and empiric experiences on the current state of ISS management inside organizations, merging these bottom-up and top-down approaches. (Figure 3).

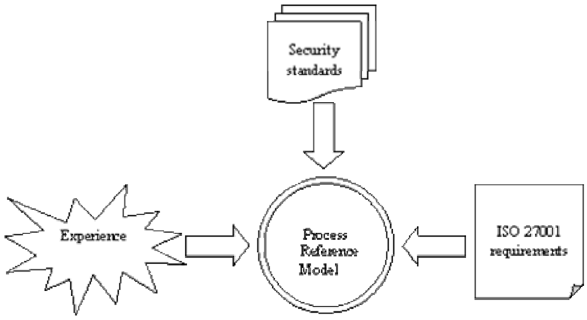


Figure 3. Design of the PRM

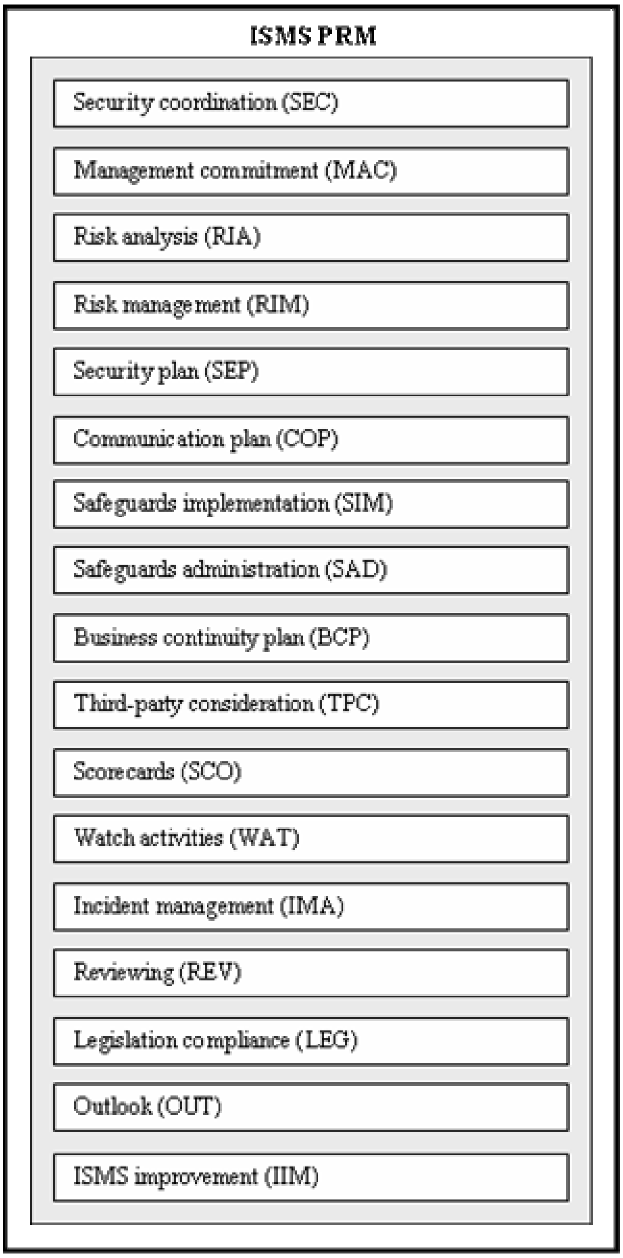
As presented above, an ISMS is an interesting innovative view for security management. Consequently, ISO 27001 requirements for establishing an ISMS have been taken into account for the PRM design. By performing every process activities of the PRM and achieving its respective goals (ISO 15504 level 1) an organization meets ISO 27001 requirements, and moreover introduces quality concepts and tools into its management for further process-oriented improvements.

However, the following fact has to be underlined. Every organization does not need nor has the necessary resources (human, time or money) to build a complete ISMS. In this case they have to consider the criticality of ICT for their business. This is especially true for little structures like SME's. In the environmental field, where EMS is the parallel of the ISMS, successful EMS implementations have been reported in organizations with only five employees, but their businesses are directly depending on environment.

Entities with business that do not rely directly on ICT also need security but require more guidance to set up a suitable set of activities. A Process Implementation Model, leading towards organizational maturity is then more relevant than process capability; this is why a PIM has been defined to provide specific guidance to implement security processes. The PIM design has been inspired by the CMMI Staged approach [24].

3.3. Process presentation

The ISMS Process Reference Model lists 17 major processes to fulfill ISO 27001 ISMS requirements. Among these processes, most of them contain a set of sub-processes to provide a more detailed guidance for security management and process-view novices. Below is the list of processes (Figure 4).



ISMS PRM

Security coordination (SEC)

Management commitment (MAC)

Risk analysis (RIA)

Risk management (RIM)

Security plan (SEP)

Communication plan (COP)

Safeguards implementation (SIM)

Safeguards administration (SAD)

Business continuity plan (BCP)

Third-party consideration (TPC)

Scorecards (SCO)

Watch activities (WAT)

Incident management (IMA)

Reviewing (REV)

Legislation compliance (LEG)

Outlook (OUT)

ISMS improvement (IIM)

Figure 4. PRM's list of processes

3.4. ISMS Process Implementation Model (ISMS PIM)

As exposed earlier, a specific guidance is needed by some organizations to set up security activities and transform them into security-concerned structures (security view), whereas other organizations with firmly implemented security practices would like to increase the quality of their processes (quality view).Both kinds of concerns must be considered. For organizations interested in the quality view, a classic process capability view is the best solution through the use of the ISO 15504 measurement framework. For those interested in the security view, an implementation model was thought. So the progressive implementation of a security policy in the context of an ISMS also aims at improving the organizational maturity. (Figure 5).

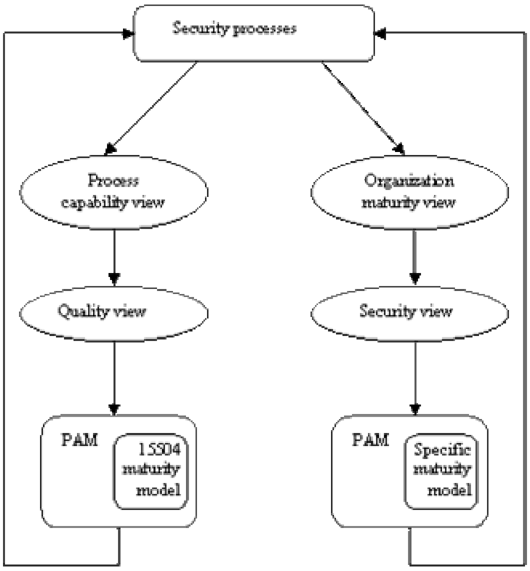


Figure 5. Which approach to choose?

This Process Implementation Model includes ten levels. Each of this level leads towards a complete accomplishment of an ISMS with the associated security policy. To reach one of these levels,, particular outcomes of the PRM's processes have to be performed (like the ISO 15504 level 1). When every particular outcome of a selected level has been met, the level is cleared and the organization could assess or implement the next one This philosophy has to remain simple because an assessment of the security practices could be conducted by both ISO15504-untrained security specialists and security-untrained ISO 15504 specialists, depending on which view (quality or security) the assessment is sponsored.

Below is a short presentation of the ten-implementation levels (Figure 6).

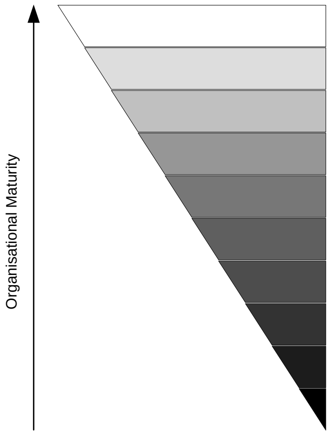


Figure 6. The pyramid of levels

♦ 0
Nothing is performed

♦ Mandatory
At this primary level, legal and regulatory requirements are met. Sufficient resources are also allocated for the security program.

♦ Ignition
First safeguards appear and represent the result of a high-level and informal thinking process.

♦ Management support
Management support is clearly established in the project. Senior management takes part in the decisional and reviewing process.

♦ Communication handling
Awareness, documentation management and inter-organization communication channels are set up to provide information to anyone concerned with ISS.

♦ Formal analysis
A detailed risk analysis is performed at this level, ensuring thoughtful decisions to be made.

♦ Verification
Specific practices take care that safeguards are correctly implemented and functional.

♦ Business protection
This level deals with business continuity. Incidents (especially the most critical ones) are managed.

♦ Follow-up

At this level, the organization has feedback on the security program efficiency and about ISS field in general.

♦ ISMS

The “We’ve done it!” level. A complete ISMS is established. All processes are performed.

4. Opportunities

4.1. The security policy

A whole set of documentation has also to be developed and maintained as suggested by the ISO 27001 to support the ISMS. As presented above, the security policy is intended to be the fundamental document when deploying a security concept within an organization. Generic models exist to help the security policy writer but 99% of them focus on safeguards and not on activities.

With a process-centered approach, the security policy needs to be written in a process-oriented way. The key idea is to enhance the role of the document and make it the heart of the ISMS, like the quality manual for a QMS (Figure 7). Each PRM selected process has to be described in terms of “What”, and completed in terms of “How” in order to address everyone, specialists or beginners in process approach and information security. The description of a security process in terms of purpose and outcomes, as defined in the ISO 15504, associated with a schedule, a financial statement and a process manager, can solve the “What” matter which particularly concerns managers and process specialists. The description of the technical and organizational procedures related to a process deals with the “How” matter to supply everyday users with clear information on how to act accordingly to the process. Only critical data have not to be included in the security policy, which raises up the topic of the security of the security policy, a fascinating one but no further discussed in this article.

4.2. Legal aspects and assurance

Another important issue in information security that addresses security managers is assurance. Towards legal aspects an organization has an obligation of means, and not of results, and therefore must demonstrate that everything reasonably possible has been performed to protect IT infrastructure and data. This is especially true when a determined organization was the relay, even unconsciously, of a cyber-attack. In some countries, like in Luxembourg, the organization could suffer from a harder sentence than the attacker himself! [26] In very ISS-concerned organization, an assurance argument is designed to prevent such consequences by making an inventory of all the security measures taken and provide it to forensics. Consequently, the security policy with all the security processes represents the assurance argument itself because it shows exactly what activities are performed or, at least, planned, by the organization to protect its information system (Figure 7).

4.3. Education

The set of security processes developed provides content for training in the field of ISS inside organizations. Beyond the ISO 27001 requirements, these processes represent an overview of activities required by ISS. The OECD Guidelines for the Security of Information Systems and Networks: “Towards a Culture of Security” [25] underlines this need for a greater awareness and understanding of security issues and practices to develop a common background among citizens, particularly ICT practitioners (Figure 7).

4.4. Benchmarking and standardization

The ISS assessment opportunities offered by the PRM enable the measurement of security capability. This measurement leads to benchmark entities for statistics purposes. These results could enable to fine tune security awareness campaigns and to define a strategy to remediate globally-observed security-flaws (Figure 7).

4.5. Assessment/certification

The assessment opportunity offered by the reference framework presented above represents an effective mean to prepare a BS 7799-2 certification (or the next to be released ISO 27001 one). Regarding standardization, the 27000th series is dedicated to ISMS-related documents. In this series, additional standards will soon appear on ISMS guidance, auditing, reviewing and metrics as defined by the ISO JTC1/SC27 roadmap. Some ideas presented in the ISMS PRM and the Process Implementation Model are going to be submitted to the SC27 working groups considering the PRM offers an auxiliary guidance for the use of the ISO 27001 standard. Luxembourg currently appraises the possibility to certify people like consultants or organizations according to this future reference framework (Figure 7).

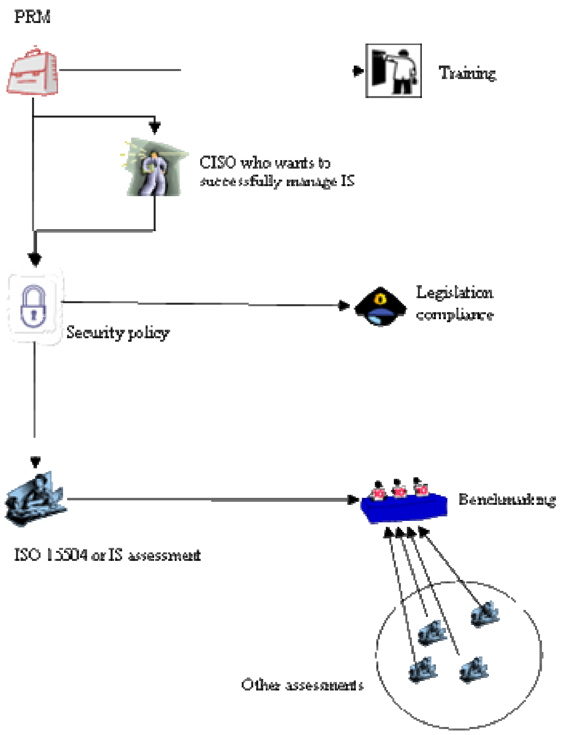


Figure 7. Security that helps everyone

4.6. Validation of the model

These ISMS PRM and PIM approaches are going to be validated through experimentation in multiple organizations. Another project of the CRP Henri Tudor (Secure- PME) is specifically dedicated to this task and to raise security practices awareness into organizations.

5. Conclusion

Security and quality are related fields. Security can be considered as a component of a quality approach, and quality as part of the risk managing framework to ensure business success, depending on the organization culture. As seen above, the quality tools can be advantageously used in ISS because they bring security activities and processes into the global organization governance. However, to be successful, awareness and training are top priorities to change people habits and win against change resistance. Moreover, quality and security have to be considered as success-enablers and no longer as cost-centres.

6. References

[1] Ministry of Economics and Foreign Trade of Luxembourg, Cyberworld AwarenesS and Enhancement structure, http://www.cases.lu

[2] Public Research Centre Henri Tudor, http://www.tudor.lu

[3] R2SIC, « Recherche pour la Sécurité des Systèmes d'Information et de la Communication », Research Project, description available at: http://www.cases.public.lu/publications/recherche/r2sic/index.html

[4] Humbert J-P., "Cybercriminality Worlds and the Social Image of the Hacker", PhD Thesis, University Paul Verlaine of Metz , France, 2004-2007

[5] Barafort B., Di Renzo B., Merlan O., Benefits resulting from the combined use of ISO/IEC 15504 with the Information Technology Infrastructure Library (ITIL), Proceedings of the International Conference PROFES'2002, Rovaniemi, Finland, 2002

[6] B. Barafort, B. Di Renzo, V. Lejeune, J-M. Simon, ITIL Based Service Management measurement and ISO/IEC 15504 process assessment : a win – win opportunity, Proceedings of the 5th International SPICE Conference on Process Assessment and Improvement, 2005

[7] ISO, ISO 15504-1: Information technology - Process assessment - Part 1: Concepts and vocabulary, 2004

[8] ISO, ISO 15504-2: Information technology - Process assessment - Part 2: Performing an assessment, 2003

[9] ISO, ISO 15504-3: Information technology - Process assessment - Part 3: Guidance on performing an assessment, 2004

[10] ISO, ISO 15504-4: Information technology - Process assessment - Part 4: Guidance on use for process improvement and process capability determination, 2004

[11] ISO, FDIS 15504-5: Information technology - Software Process Assessment - Part 5: An exemplar process assessment model, 2005

[12] Hoyt Douglas B., Bosworth S., Kabay M. E., Computer Security Handbook, John Wiley & Sons, 2002

[13] Direction Centrale de la Sécurité des Systèmes d'Information, Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) version 3, available at : http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html, 2004

[14] Carnegie Mellon University, Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE), available at: http://www.cert.org/octave/, 2001

[15] ISO, ISO 7498-2: Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, 1989

[16] ISO 13335-1: Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management, 2004

[17] ISO, ISO 17799: Information technology - Security techniques - Code of practice for information security management, 2000

[18] Poggi S., Veille sur les standards et méthodes en sécurité, available at : http://www.cases.public.lu/publications/recherche/r2sic/wp11_1.pdf, 2005

[19] Chardonnet A., Thibaudon D., Le guide du PDCA de Deming - Progrès continu et management, Editions d'Organisation, 2003

[20] BSI, British Standard 7799-2: 2002, Information Security Management Systems – Specification with guidance of use

[21] ISO, ISO 9001: Quality management systems – Requirements, 2000

[22] ISO, ISO 14001: Environmental management systems - Requirements with guidance for use, 2004

[23] ISO, ISO 27001: Information technology - Security techniques - Information security management systems – Requirements, 2005

[24] Carnegie Mellon University, CMMI^{SM} for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing, Version 1.1, Staged Representation, 2002 available at : http://www.sei.cmu.edu/publications/documents/02.reports/02tr012.html

[25] Penal and civil code of Luxembourg, available at: http://www.legilux.lu

[26] OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, available at: http://www.oecd.org/dataoecd/16/22/15582260.pdf, 2002

DCSSI, Meilleures pratiques pour la gestion des risques SSI, exploitation des résultats de la méthode EBIOS dans le cadre d'une démarche BS 7799, available at: http://ebios.cases-cc.org/fr/3-MeilleuresPratiques/EBIOSv2-MP-BS7799-2003-03-21.pdf, 2003 (revision next to be published)

Viral S., Costs and Benefits of using Smaller Assessment Models for Software Process Assessment and Improvement in Small Software Organizations, Proceedings of the 5th International SPICE Conference on Process Assessment and Improvement, 2005

Barafort B., Di Renzo B., Assessment and improvement integrated approach: combined use of the ISO/IEC 15504 (SPICE) and the Information Technology Infrastructure Library (ITIL) , Proceedings of the National Conference SPIRAL'2004, Luxembourg, 2004

Picard M., Lejeune V., Modélisation des processus ITIL à l'aide d'autres démarches qualité, Facultés Universitaires Notre-Dame de la Paix, Institut d'informatique, Namur, Mémoire présenté en vue de l'obtention du grade de Maître en informatique, 2004