December 2007

ISO Security Standards as a Leverage on IT Security Management

Igli Tashi
Business School-Lausanne University

Solange Ghernaouti-Hallie
Business School - Lausanne University

ISO security standards as a leverage on IT Security Management

Igli TASHI, Research assistant
HEC Business School –University of Lausanne
Switzerland
Igli.Tashi@unil.ch

Solange GHERNAOUTI-HÉLIE, Professor
HEC Business School –University of Lausanne
Switzerland
sgh@unil.ch

Abstract

Information security is a very important component in the context of an organization's dependence on ICT. The operational environment where these technologies are operating is a very complex one. Offering a good level of protection by information security process needs a well defined managerial framework.
This paper discusses the reasons why having a well defined managerial security framework is needed in an information security area, as well as which are the tools to build and implement such a management framework. After a short presentation, two international standards related to Information Security Management, the ISO 17799:2005 and ISO 27001 standards, and the implications of being conforming to these standards are analysed and their advantages and limits in a security management framework are pointed out.

Keywords: *Information Security Management, Risk Management, Information Security Management effectiveness/efficiency, Information Security Management complexity, Quality Management, Compliance and Conformity, ISO 27001 and ISO 17799 standards impact on IT security management.*

1 – Managing IT security as a complex task

Technology is the main factor for productivity growth and organizations' competitiveness that allows effective cost reductions. The use of technologies, their role and importance are increasing more and more each day. The current hefty globalisation and de-localization phenomena should not be ignored any more. If we analyse the constitution of the most companies referenced in the Forbes' Global 2000[1], which are considered as being the most important companies in the world-wide market, we immediately realize that it features some huge and

[1] http://www.forbes.com/2003/07/02/internationaland.html

multinational constructions with wide spreading activities. Many of these companies comprise a number of subsidiary companies everywhere in the globe dealing with different business models, cultures and issues. This model becomes more and more prominent in the market structure by the means of mergers, coalitions, acquisitions etc. In the core of such a global and complex structure, information takes a very important place and becomes a critical asset that needs to be protected. Companies rely more and more on computer and network systems to conduct their business. In that way, ICT governance become important for the companies' durability and ICT security management has to be integrated in the whole organizational management program.

1.1 – Why is managing ICT security a complex task?

Managing ICT security in such a dynamic and chaotic operational environment is a very difficult task for security practitioners. First of all, every managerial process, security related or not, begins by defining the boundaries of the system that needs to be protected. In the information security domain, taking into account the very complex operational environment, a system's boundary tends to be blurry. But , more importantly, even if a company fixes the boundary and the assets to be protected inside the boundary, a breach occurring outside could have an adverse impact in the structure's core. For example in a multinational corporate having numerous and interrelated subsidiary companies located all over the world, a security breach to one of these subsidiary companies could permit intruders to enter in the main system of the parent company.

1.1.1 – Interdisciplinary requirements for Information Security

A main concern in the ICT security management area is that security managers have to deal with multiple subjects (technical, economical, ethical, legal, and managerial) which represent multiple issues to be resolved in multiple ways. Security issues are among those rare organizational issues that require the mobilization of all the organization's resources and involved parties.
ICT security management has to work on:

- some business functions like policies, standards, procedures involving a lot of stakeholders such as policy team, compliance department, human resources department, IT department, etc.
- some operational stages which include tests and controls, physical and organizational safeguards, incident handling involving developers, system administrators response team, project teams, etc.
- some assurance processes like auditing, knowledge and awareness processes involving auditors, trainers, experts, etc.

The security architecture has to integrate a great number of components like technical, human, organizational and legal ones. It has to fulfil a lot of functions on many levels absorbing a significant part of the organisation's skills and resources.

1.1.2 – Information Risk's components

The complexity arises from the nature of the risk. Informational risk is continuously changing due to the changing nature of its components. A risk function can be defined by the following equation:

$$RISK = F\ [threat,\ vulnerability,\ impact];$$

Every change in any of the independent variables will affect the dependent one, the risk.
The subcomponents of the *Threat* variable are too great in number to be considered and so are countermeasures to be put in place. Examples to be mentioned are social engineering, errors, omissions, disclosures, denial of service, unavailability, frauds etc.
The second of the risk's component, which is the core of the problem, is *vulnerability*. Vulnerabilities are innumerable for many reasons and discussing their whole range is not in the scope of this paper. According to

Common Vulnerabilities and Exposures[2] catalog there are some 23578 known and inventoried vulnerabilities. Nevertheless, we should mention here the most important one, which derives from the way information system components and technologies are commercialized. It is related to the pressure a producer faces in order to be the first one proposing solutions and products to the market. Such pressure induces a producer not to take the time necessary to assess security components of their product. In that way, users become a kind of beta testers using vulnerable products during a time which is not insignificant.
The *impact* is another complex component of information risk. Information risk menace principally intangible assets and it is rather difficult to specify their value. First of all, companies do not have an exhaustive inventory with a well-specified financial worth. Secondly, the financial worth of an informational asset is subjective according to its owner's perception. Therefore this informational asset should be evaluated according to its criticality and sensitivity within the company's business framework.

Another complexity issue arises from the network connectivity. In this respect, a company is vulnerable not only as a consequence of its own behaviour but also because of that of others. Being connected to a complex operational environment[3] exposes companies to interdependent risks which are rather difficult to identify and qualify.

A risk management process has to consider all of risk's components in order to choose or to propose the most appropriate countermeasures. Being concerned by cost that countermeasures generate, security managers have to make a cost-benefit analysis in order to spend limited resources appropriately to get good results.

1.1.3 – Compliance issues

Several regulations have emerged during the last years. Without pretending to be thorough, we can mention Sarbanes-Oxley Act, Basel II accord, Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), EU's Privacy and Electronic Communications (Directive 2002/58) and the Data Protection Directive (Directive 95/46/EC). These laws have certain key concepts in common like accountability, protection of personal private information, disclosure of disclosure policies and integrity of reported information. Many sorts of organizations are concerned by these regulations which define some requirements concerning informational risk without specifying them in a more detailed way.
Many organisations find the need for compliance to be a catalyst in resolving long-overlooked security problems but at the same time, the need to satisfy regulatory requirements increases the complexity level of the IT security management process.

1.2 – Managing a complex task in a quality management framework

Taking into account the considerations we made, managing information security issues is a rather complex process. According to the ISO 9000:2005[4] standard, a process is defined as a set of interrelated or interacting activities, which transform inputs into outputs as shown in figure 1:

[2] Source http://cve.mitre.org/
[3] See Carralli, R.A., & Wilson, W.R. (2004)
[4] See ISO 9000:2005 «Quality management systems -- Fundamentals and vocabulary»

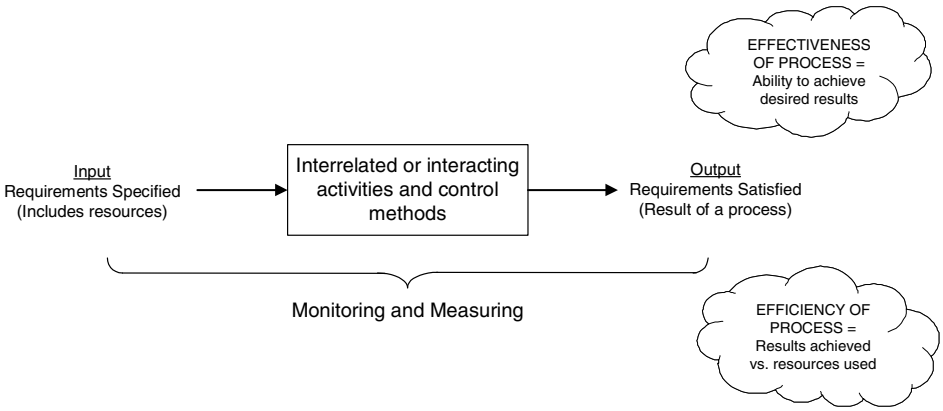

Figure 1: Generic processes; Source: http://isotc.iso.org/

Information security was previously considered as a technical discipline. For that reason information security processes predominantly focus on risk mitigation confirming technical vulnerabilities. [5] Threats like viruses or unauthorized access to information making up respectively 65% and 32% of attacks detected in a period of 12 months[6] should not be purely countermeasured by technical means such as antivirus software or firewalls. Virus contamination or unauthorized access to information arises from a misuse of these technologies rather than from insufficient technical quality. In the case of viruses the breach's origin is the fact that the some forgets or aborts an automated procedure to update the software. Such kinds of issues are typically rectified by a well-defined managerial process rather than the degree of skilfulness.

The current reality concerning information security has changed because of many factors[7]:

- The rapidly increasing size of interconnected networks and the Internet as a whole;
- New networking technologies;
- Hardware and software' heterogeneity;
- The increased interdependency between business processes and IS products;
- The accelerated development of new technologies which forces companies to restructure their IT systems, etc.

This complex environment involves a multiple number of procedures, activities and controls. Furthermore responding to the increasing number of threats and vulnerabilities requires a great number of solutions for which besides their effectiveness and efficiency a manager has to evaluate their cost benefit ratio. As we have already mentioned, this environment is interdependent and interoperable, hence an increased need of management framework and skills arises.

The problem is that information security has to take care of all these issues taking into consideration the constraint that an organisation's security system is as strong as its weakest link. So every process, component, tool, activity has to be considered with the same intention.

Managing the complex domain of information security requires a well-defined methodology and proceeding. On the other hand, considering the interoperability and interdependent variables the required methodology has to be largely shared by the involved parties and express the same shared understandings of what a information security management framework has to look like, which are the areas to be considered and which are the proceedings to meet the organisation's security goals and requirements.

This leads practitioners to build up some guidelines and standards to better follow and unify the different practices encountered within the information security domain. ISO responded to this need by defining some standards related to information security management, which are *ISO 17799:2005 Code of practice for information security management and ISO 27001 Information security management systems – Requirements*

2 – International security standards as a tool to decrease Information's Security Management complexity

[5] See Blakley, B., & McDermott, E., & Geer, D. (2001)

[6] See Computer Security Institute & Federal Bureau of Investigation. (2006). *Computer crime and security survey 2006*

[7] Adapted from: Herrman. K., & Mühl. G., & Geihs. K. (2005)

Following a short presentation of two international standards related to Information Security Management, ISO 17799:2005 and ISO 27001, the implications of conforming to these standards are analysed and their advantages and limits in a security management framework are pointed out.

2.1 – Presentation of international standards

2.1.1 – ISO 17799:2005 Code of practice for information security management

In the 90's, the representatives of some large companies like Shell, British Telecom, Marks & Spencer defined a "code of best practices" according to their experience. This document was taken up again and published by British Standard Institute (BSI). In 1995 the first BS 7799 standard appeared, under the title "Code of best practices for information security management". This document was passed to ISO to be standardized under the named ISO 17799:2000 Code of practice for information security management. Since then, a new version of the ISO 17799 (BS-7799: part1) was published in 2005 (ISO 17799:2005.) This standard contains recommendations which contribute to the information security management by taking into consideration the persons in charge of the definition, implementation or maintenance of organizations' information security. It constitutes a common base of development of the information system security. The ISO standard defines the information security as the protection of the availability, integrity and confidentiality of the information assets irrelevant of these being in a written, spoken or digital form. It aims to ensure the business continuity, the damage reduction, but also to maximize the return on investment of Information Systems. The ISO 17799 standard is an approach based on the risk management, to plan out a suitable policy, procedures and controls in order to better manage IT risks. This process is balanced between physical security, technical security, procedural security and human related security (figure 2). The assets managed by this standard are the informational assets like files, databases, records, the physical assets (servers, PC, laptops, computer hardware), software assets and the assets related to the services (informatics and communication departments, general services, power supply) etc.

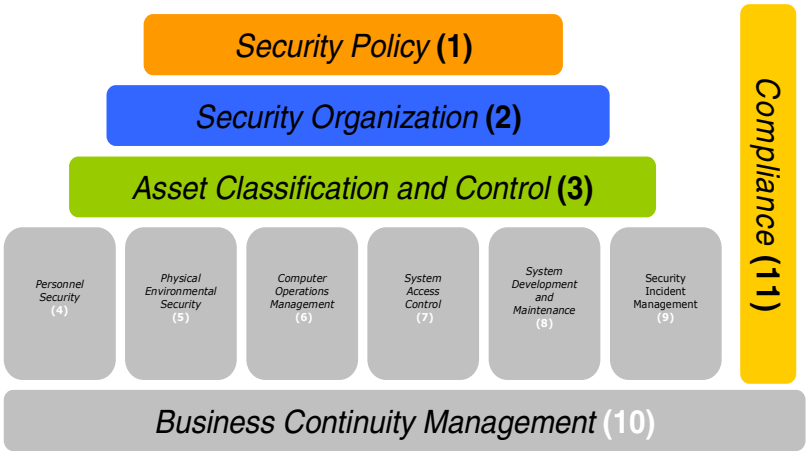

Figure 2 : ISO 17799 :2005 chapters

The ISO 17799:2005 standard comprises 11 chapters[8] as outlined in the figure above. In the current version one more chapter, named "Security Incident Management", is added in comparison to the ISO 17799:2000 standard.

[8] See International Standards Organization. (2005). *ISO/IEC 17799:2005, Code de bonne pratique pour la gestion de la sécurité de l'information*

2.1.2- ISO 17799 and methodologies

Aside from the ISO 17799:2005 standard, several methods exist such as MEHARI, EBIOS, OCTAVE, ITIL that attempt to assess the IT risks. There is a method named CobiT (Control Objectify for Information and related Technology) which can also be apprehended as a security reference framework which treats several topics related to the information security management. Indeed, CobiT is an audit related best practice. CobiT (the 4th edition) helps management to establish a link between the business risks, the needs for control and the technical problems. CobiT constitutes a complete reference frame making possible to put under control the whole of information systems related operations. CobiT comprises 34 Control Objectives of System gathered in four broad fields (figure 3):

1. Plan and Organise
2. Acquire and Implement
3. Deliver and Support
4. Monitor and Evaluate

The goals pursued by this method are similar to those of the ISO 17799 standard. The difference is the classification between a standard and a method. Indeed, an international standard is developed by international standards organizations. By definition, international standards are suitable for universal, worldwide use and they cover large industrial and economic interests and are established in a voluntary process. On the other hand, a method is an instrument to reach effectively a precise desired result. A method does not integrate the reference document concept or the consensus concept. In general, a method is the tool used to satisfy a standard.

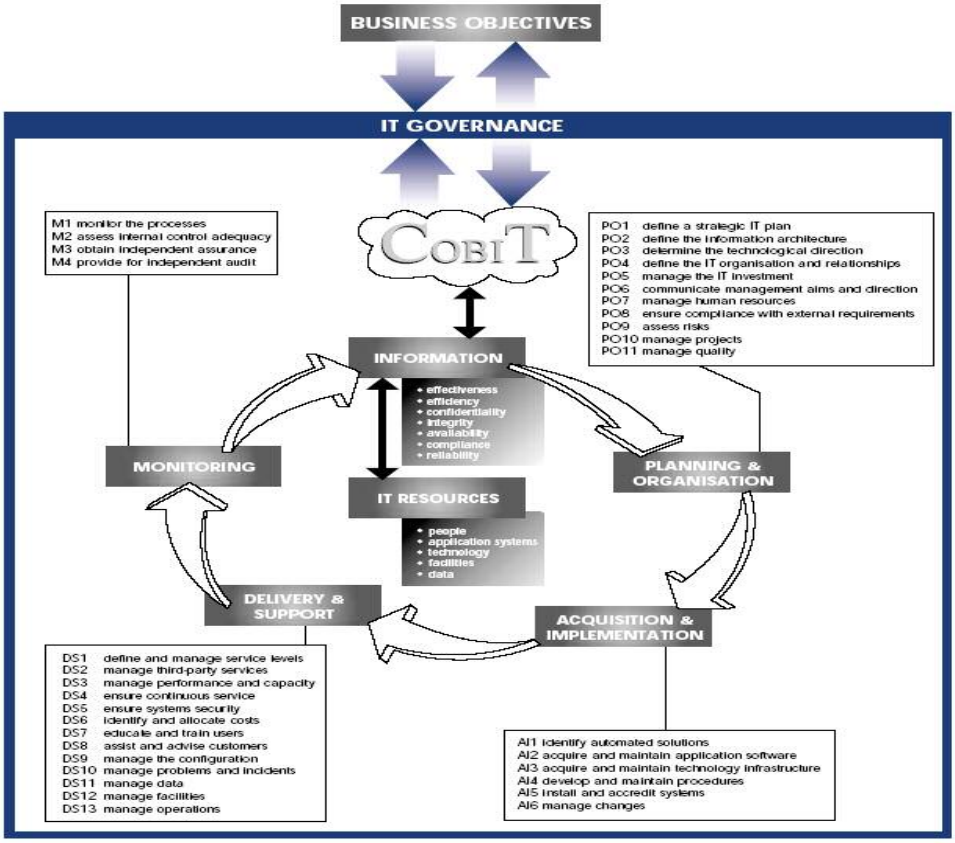

Figure 3 : CobiT IT processes defined within the four domains

2.1.3- ISO 27001 Information security management systems – Requirements

The ISO 27001 standard (Information Security Management System) goes into the same direction and contains the same objectives as ISO 17799. This standard corresponds to BS 7799. The ISO 27001 standard concerns all the industry and trade sectors. The difference is that ISO 27000 is a standard that anyone can be certified to, in opposition to ISO 17799 which is a standard of "best practices" concerning information security.

Developing an ISMS meeting ISO's 27001 requirements implies having three stages (figure 4):

1. The first stage is related to the creation of a managerial framework concerning the information system. It is about defining the directives, intentions and objectives related to information security and at the same time laying down the strategic policy which would engage the top management's responsibility.
2. The second stage is related to the risk identifications and evaluations according to the organization's security requirements in order to define the proper managerial actions to undertake. The aim is to define priorities to control the information security risks.
3. The last stage is related to the development of an ISMS and thus, to the selection and implementation of controls to be carried out. Indeed, once the requirements are identified, adapted controls can be selected. These controls must ensure that IT risks are assessed, mitigated and by this reduced to an acceptable level for the organization. These controls are related to policies, practices or proceedings to be followed considering the organisations' structure.

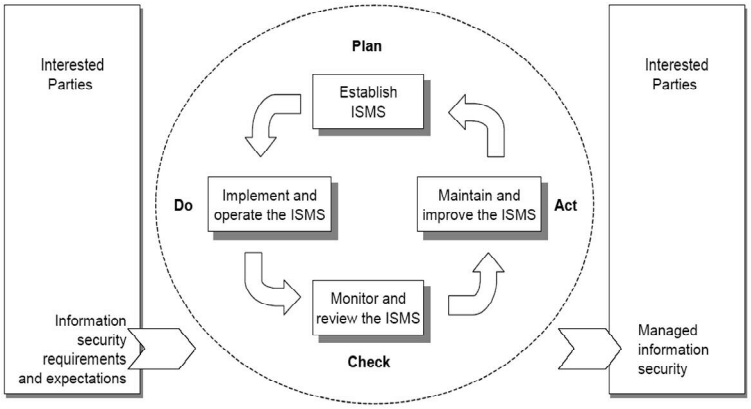

Figure 4 : PDCA model applied to ISMS processes

The ISO 27001 standard proposes and details the implementation and the documentation required for an ISMS. ISMS is the approach proposed by ISO 27001, to validate and document the existence of a managerial approach concerning the information security management, being completed by certification proceedings. An ISMS is conceived in a way to ensure that adequate and proportional security controls are selected. This standard is increasingly used by organizations as shown in figure 5:

Japan	2043*	Austria	11	Oman	2
UK	329	Saudi Arabia	9	Pakistan	2
India	285	Spain	9	Slovak Republic	2
Taiwan	127	Philippines	8	South Africa	2
Germany	74	Sweden	8	Sri Lanka	2
Hungary	57	UAE	8	Armenia	1
Korea	49	Iceland	7	Bulgaria	1
USA	48	Greece	5	Gibraltar	1
China	47	Kuwait	5	Egypt	1
Italy	43	Russian Federation	5	Lebanon	1
Australia	42	Thailand	4	Lithuania	1
Netherlands	31	Argentina	3	Luxemburg	1
Singapore	28	Bahrain	3	Macedonia	1
Hong Kong	26	Canada	3	Moldova	1
Czech Republic	25	Croatia	3	Morocco	1
Malaysia	19	France	3	New Zealand	1
Poland	17	Indonesia	3	Peru	1
Brazil	15	Isle of Man	3	Qatar	1
Ireland	15	Macau	3	Serbia and Montenegro	1
Switzerland	15	Romania	3	Ukraine	1
Finland	14	Slovenia	3	Uruguay	1
Norway	14	Belgium	2	Vietnam	1
Turkey	13	Colombia	2		
Mexico	12	Denmark	2	**Total**	**3530**

Figure 5 : Number of certificates per country*, Source : ISMS International User Group*

2.2 –International Standards' impact on Information Security Management area

The ISO 17799:2005 standard provides some guidelines and some general principles regarding the way to prepare, carry out, maintain and improve information security management within the organisation. Every chapter shown in figure 2 consists of several sections. Every section includes a security goal, some measures which can be applied to achieve the security goal and the way to implement them.
In contrast, the ISO 27001 standard provides a model for establishing, implementing and maintaining an Information Security Management System. In other words, the ISO 27001 standard states the way the security information management mechanism and the guidelines proposed in ISO 17799 have to be built up and implemented, the way the ISO's 17799 recommendations have to be put in place.
According to what was shown above, most of security practitioners concur with the idea that having a good level of information security requires a good management framework. The importance of management to improve information security quality and the need for a standard was recognized by the early of '80 as shown in 6:

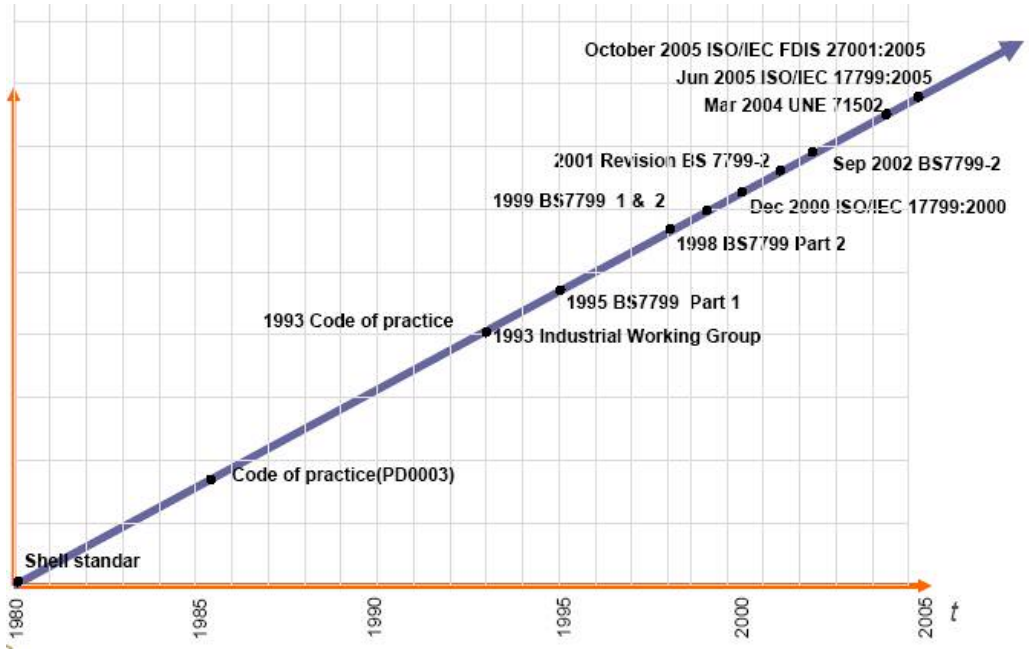

Figure 6- Information security related best practices' evolution
Source: http://www.certconf.org/presentations/2006

Principally, the impact of ISO's standards resides in the way this management framework has to be built up. This begins with the topics that this framework has to include based on the statement that information is an assets (principally intangible) and as such, like other important business assets, is essential to an organisation's business and needs to be suitably protected. The management framework must include all activities and involved parties on this protection and not only technical aspects. The ultimate purpose of such a management framework is to minimize the information risk and doing this requires considering all of risk's dimensions, that is to say threats, vulnerabilities but also an organisation's security requirements and security controls based on the assets value and the business impact of a security breach.
The other step was to state, which are these domains to be included in such a security management framework. Security management passes form a single technical issue consideration to an overall security concept related to a quality and culture concept. Much consideration was dedicated to the security policy which is a definition of what it means to be secure for an organisation, provides guidelines to users on the processing, storage and transmission of sensitive information and ensures that information is appropriately protected. Besides that, it manifests the top management's commitment to information security and places information security responsibility at a higher level. Information security is not only a matter of IT department engineers, but it should be a matter of everyone acting within an organisation. With information being considered as an asset, even a very important one, responsibilities related to its protection has to be assigned. The human factor was placed in the core of information security and a great importance was given to the management of human resources. Different international and national regulations and accords classify informational risk as an operational one. So users must understand their role in information security and being conscious about their responsibilities. On a higher level, security functions concern not only specialized people but a larger group including senior management, business and functional managers, system and information owners and of course senior management.

Another important impact of the standard in the security management framework was the fact that an organisation has to take into account the regulatory domain. Risk is perceived in two different ways, that is to say the harm of a security breach within the organisation and his incidence for the third persons. A new important and non technical risk appears which is needed to be taken into consideration.

2.2.1 –Standard's impact on IT security management framework

The application of the ISO17799:2005 based on a risk management assessment approach gives some guidelines regarding Information Security Management and it is a description that is currently considered important. The standard focuses on the principal problems concerning the information security issues and gives some recommendations about the way to better manage the information assets by categorising potential risks. It goes deeper into the corporation culture and shows that security awareness is an important component within the organization. The standard does not consider information security as a technical discipline and fills the gaps in previous ways of thinking in information security

The standard's application as well as the fact of being in conformity with it contributes to the information risk control and mitigation, making organizations responsible for their informational asset importance. The standard could be used to develop procedures and solution implementations to protect these assets. Organizations will be more conscious of the measures to be taken in a total and systemic manner. Thus, a specific security reference frame could be built and organizations would be able to communicate their security strategy in an easily and comprehensible way. According to this fact, we have to focus on our intention about the security domains to be considered, in order to assess in a better way the organizational security preparedness. As it is showed on Fig. 2, ISO 17799 considers that the 11 domains represented are very important for the effectiveness/efficiency of the information security.

One of the greatest interests to use the ISO 17799:2005 standard resides in its international recognition, due to its status as an ISO standard. Originally impugned, it seems that this standard is increasingly adopted by organizations. The use of the ISO 17799:2005 standard allows for simplifying the use of security methods as well as for communication between companies, and in addition promotes the use of a common language. This allows facilitating security comprehension and apprehension by all parties involved. In order to remain competitive in a global economy structure, organizations must be restructured by trade issues rather than by country.

On the other hand ISO 27001 provides a process based approach and requirements for continuous improvement cost-effective information security solutions. The standard assesses and controls the informational risk related to a strategic business plan and an operational environment. It is a very important risk management tool and reference frame. Achieving information security according to ISO 27001 is implementing a set of controls based on a risk assessment approach regarding policies, practices, procedures, organizational structures and software functions.

Obtaining a third party certificate attests that you have treated, implemented and controlled the information security. This means that you are interested in building a security culture within the organisation increasing security awareness. This allows the organization to be positioned in the competitive market. Amongst others, certification makes it possible to inform and consolidate the stakeholders about the way organizations' information system is protected. That can lead to increase an organizations' credibility and confidence level. Additionally, certification leads to a cost cut because certification contributes to the reduction of incidents' frequency and thus reduces costs associated with their impacts. Certification does not certify for a "security level" but for the way IT risks are managed within the organization. More specifically, ISO's 27001 certification attests that the organization has put in place some proceedings and an information security management system as well as a risk analysis system. Following this, the standard certifies the relevance and the effectiveness of the implemented resources. The ISO standard within Appendix A proposes 134 controls shared out into 11 topics concerning all these aspects.

3 – Conclusion: Some issues from standard's effectuation

Do ISO's security management standards allow reaching a high security level?

It helps a lot; there is no doubt on that. But how do the ISO's standards requirements tailor to a specific organization?

We stated within this paper that informational risk and the way to assess it is a matter of perception and having a good level of information security management will depend on this perception.

Satisfying ISO 17799:2005 requirements only shows due diligence but not the outputs' effectiveness. This standard is a check list of some procedures and controls to be implemented which emphasise on conformity and

as it is shown in figure 1 the required output of a process aside from the conformity should be effectiveness and efficiency.
ISO 27001 provides a model for establishing, implementing and maintaining an Information Security Management System. The question to be posed is: Does this ISO's 27001 conform security management system work in its best possible way?

Being conform to a standard is a good starting point. Many companies selling ISO conformity exist in the market which is apparently a good business. But there is an ambiguity about the "conformity" they sell. In fact they sell counsels for how to build security policies or how to evaluate the organization's security process complying with ISO security standards framework. It is some kind of consulting work which treats security issues in a very generic way.

Security managers need to produce effective security, as following standard by itself is not sufficient. ISO standards give directives but do not specify their effectiveness or how a security level can be achieved. A larger set of tools is needed in order to achieve the principal goal which is a better security level.

Information security driver is to build confidence into ICT infrastructures. Being in conformity with a standard is producing confidence into security? This is another question we have to respond when we consider an IT security management process. Expressing confidence by conformity is not sufficient; it must be linked to the quality of the system.

Satisfying the ISO 17799:2005 and 27001 requirements does not show the way to build the management system at the moment. Complying with a standard does not mean going into depth. As we have seen, information security is an ongoing process realized in a dynamic environment while conformity (or certification when it exists) is only valid for a static state of a process or component. Conformity does not integrate the mandatory anticipation dimension of the security management process required by the evolving nature of IT risks.

At present, the trend is to state that the organisation is right if it complies with specific regulations and standards. It is mostly a legal protection but it does not produce IT security. Legal and regulation constraints should be seen as key factors to oblige the organisation to put in place an effective information security management framework. To do that ISO Standards could help, but one should keep in mind that an organization's competitiveness depends on its security effectiveness and that it is not conformity which guarantees security effectiveness.

References

- Blakley, B., & McDermott, E., & Geer, D. (2001). Proceedings from New security paradigm workshop: *Information security is Information Risk Management.* Cloudcroft, New Mexico: ACM Press
- Calder, A. (2005). *The case for ISO 27001*. UK: IT Governance Publishing.
- Carralli, R.A., & Wilson, W.R. (2004) *The challenges of Security Management », software engineering institute*. Retrieved February 15, 2006 from http://www.cert.org/archive/pdf/ESM**challenges**.pdf
- Club de la Sécurité de l'Information Français. (2003). *ISO 17799:2000: une présentation générale*. Retrieved February 15, 2007 from http://www.clusif.fr
- Club de la Sécurité de l'Information Français. (2006). *Politiques de sécurité des systèmes d'information et sinistralité en France*. Retrieved February 15, 2007 from http://www.clusif.fr
- Cohen, F. (2006). *IT security governance Guidebook with security program metrics*. US: Auerbach Publications
- Computer Security Institute & Federal Bureau of Investigation. (2006). *Computer crime and security survey 2006*. Retrieved February 10, 2007 from http://www.gocsi.com

- Ghernaouti, S. (2006). *Sécurité informatique et réseaux : cours et exercices corrigés*, France : Dunod
- Herrman. K., & Mühl. G., & Geihs. K. (2005). Self management: The solution to complexity or just another problem ?. *IEEE distributed systems online,* 1541-4922. Retrieved January 20, 2007, from http://csdl2.computer.org/comp/mags/ds/2005/01/o1001.pdf
- Hutt. A., & Bosworth. S., & Hoyt. D. (1995, 3d edition). *Computer Security Handbook*. US: John Wiley & Sons, Inc.
- International Standards Organization. (2005). *ISO/IEC 17799:2005, Code de bonne pratique pour la gestion de la sécurité de l'information*. Retrieved May 05, 2006 from http://www.iso.org
- International Standards Organization. (2005). *ISO/IEC 27001, Information security management system-Requirements*. http://www.iso.org
- Jones A., & Ashenden D. (2005). *Risk management for computer security*.UK: Elsevier.
- Kajava J., & Savola R. (2005). Towards Better Information Security Management by understanding Security Metrics and Measuring Processes. University of OULU Finland, cahier n°02 – 2001. Retrieved January 20, 2007, from http://www.mc.manchester.ac.uk/eunis2005/medialibrary/papers/paper_154.pdf
- Landoll. D.J. (2006). *The security risk assessment handbook.* US: Auerbach Publications
- National Institute of Standardization and technology. (2002). *Risk management Guide for Information Technology Systems.* Retrieved February 15, 2007 from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Nelson. A. (2007). ISO 27001 as a Support to Digital Forensics. *Journal of Digital Forensic Practice,* 1:1 43-46. Retrieved Avril 25, 2007, from http://taylorandfrancis.metapress.com/index/Q17W1X8PK26M1474.pdf
- Secretariat of ISO/TC. (2004). *ISO 9000 Introduction and support package: Guidance on the Concept and Use of the Process Approach for management systems.* Retrieved February 15, 2007 from www.iso.org/tc176/sc2
- Su, X., & Bolzoni, D., & van Eck, P.A.T. (2006) *A Business Goal Driven Approach for Understanding and Specifying Information Security Requirements.* Technical Report TR-CTIT-06-08 Centre for Telematics and Information Technology, University of Twente.
- Whitman. M. E., & Mattord. H. (2007). Management of Information Security. US: Course Technology