Strengthening the Management of Ubiquitous Internet by Refining ISO/IEC 27001 Implementation Using a Generic Responsibility Model

Christophe Feltus and Djamel Khadraoui

Public Research Centre Henri Tudor

2017

Strengthening the Management of Ubiquitous Internet by Refining ISO/IEC 27001 Implementation Using a Generic Responsibility Model

Christophe Feltus, Djamel Khadraoui
Public Research Centre Henri Tudor
Luxembourg - Kirchberg

Abstract

The recent emergence of decentralized networks and ubiquitous Internet has highlighted the need for a better management of the companies' IT architecture and for an improvement of the users of the network's responsibility. Many standards have recently emerged to face these requirements. By analyzing them, we observe that they all include reference to the user responsibility but also that no common understanding of it exists. These statements have oriented our research toward the elaboration of an innovative, simple and pragmatic responsibility model that includes a user commitment dimension.

ISO/IEC 27001:2005 is one of that new standard that aims at providing a framework for improving the information system management and the security of IT architecture. Although this standard is recognized over the globe, many surveys and cases studies provide interesting feedback about its implementation problems. In this paper, we introduce our responsibility model, we depict the responsibility aspects encompassed in ISO 27001 and we propose some improvement perspectives to face these problems and strengthen its implementation.

Keywords: Responsibility, Capability, Accountability, Commitment, ISO 27001, Access rights.

1. Introduction

Ubiquitous Internet has request for a global rethinking of companies IT architectures. Industrial analyses as well as academic surveys have put forward the need for improving the governance of these architectures. This need is, in practice, translated in a considerable amount of requirements such as more transparency, more control, more alignment with the business and more suitable definition of the responsibility of the employees that use these architecture. This last requirement is beside the first of the six principles of the new standard for Corporate Governance of IT: ISO/IEC 38500:2008 [1].

In parallel to those newly arising and progressively formalized requirements, companies are used to work with well-known, experienced and approved management frameworks within their day-to-day operations, management, or investments. These frameworks are i.e. COBIT [3], a framework that enables the development of clear policies and good practice for IT control throughout enterprises, IT Infrastructure Library (ITIL) [2], a public library that focuses on IT services management for high-quality service provision, CIMOSA [4], an enterprise architecture model to define industrial computer system architecture or the international standard ISO/IEC 15504 [5]. By depicting the concept of responsibility in all of that frameworks, we observe that this concept is used in all of them, but it exists no consensual and unique meaning of it.

As consequence, we have oriented our work toward firstly the elaboration of a unique and consensual responsibility model and secondly the confrontation of that responsibility model again these existing frameworks.

The research method used to develop this model is a two steps approach. In step 1, we depict the scientific literature in the field of responsibility to identify its main conceptual components. In step 2, we elaborate a UML responsibility model based on the component found in step 1 and we operate successive refinements by comparing it with existing professional management framework.

Thereafter, we focus our research on the standard ISO/IEC 27001:2005 (ISO 27001) [7]. This standard has a paramount significance for the security management of ubiquitous computing because it aims at implementing a proactive management system adaptable for open architecture. By analyzing it, we however observe that it is a twelve-pages standard, accompanied by three annexes. Only six pages of it include information really dedicated to the management of the information system (IS): ch.4.2 and ch.5, resp. "*Establishing and Managing the ISMS* and *Management Responsibility"*. Although the standard's synthetic character is probably one reason of its worldwide recognition, there is no doubt that it also may lead to misunderstanding and misinterpretation. Surveys of its implementation [8] highlight that recurrent problems arise and we will explain in this paper how they could be reduced according to a better interpretation of responsibility elements.

In chapter 2, we will first introduce arising problems and challenges regarding ISO 27001 implementation. Afterwards we will propose an innovative responsibility model and explain some of its most important components based on the literature review and previous works. Finally, we will analyze 27001 compared to our responsibility model perspectives and highlight how some implementation challenges could be faced.

2. Implementation Problem

ISO 27001 is an international standard aiming to:

"[…] specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS (Information Security Management Systems) within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof." [7]

Due to its international success, ISO 27001 has been subjected to a profusion of implementation reports, case studies and surveys [8] [10] [33].

One of these interesting surveys, produced by Certification Europe Survey [8], gathers information collected over a 4 months period in 2007 to analyze how ISMS managers in organization certified ISO 27001 has perceived the implementation stage of the standard. The survey has been achieved by a questionnaire having been completed by 312 managers from all around the globe: India, Ireland, Italy, Hong Kong, Japan, UK and US. Companies of the IT services' area and software development, followed by telecom companies, provided most of the answers, with respectively 23% and 14%. Surprisingly, the financial sector only provided 3%. Companies with less than 200 employees answered at a rate of 27%.

The survey provides an interesting input regarding the three most important challenges to face during the implementation and consequently, the risk of failure to reduced:

1. Having an ISMS implemented means an important cultural change within the organization. This change is a serious brake that needs to be taken into consideration to be apprehended.
2. Senior management buy-in (or commitment) is a real factor of success for the implementation of ISO 27001. However, the survey highlights that in a number of case studies this commitment tends to disappear after some months following the beginning of the implementation.
3. Finally, the lack of resource is to be followed up.

3. Responsibility Model

The elaboration of the model has been realized according to a double activity. First, we have constructed a theoretical model based on the analysis of its conceptual components issued from incomes of the social, managerial, psychological and computer sciences literature. Secondly, the theoretical model has been enhanced and validated by confrontation with

industrial frameworks. Simultaneously, these existing industrial frameworks have been improved by adjunction of conceptual components from the responsibility model, i.e. [9] [11] [12].

The **responsibility** concept analysis [13] highlights the existence of a plethora of definitions. We may however state that commonly accepted responsibility's definitions encompass the idea of having the obligation to ensure that something will happen. Our previous works have led to the construction of the model illustrated in Figure 1. This model addresses the following three responsibility's concepts' blocs: the *accountability* of the responsible person regarding his obligations, the *right* necessary to assume the responsibility and the affectation process [31] [32] requesting the employees' *commitment*. In this paper, the affectation process will be closely associated to the delegation mechanism.

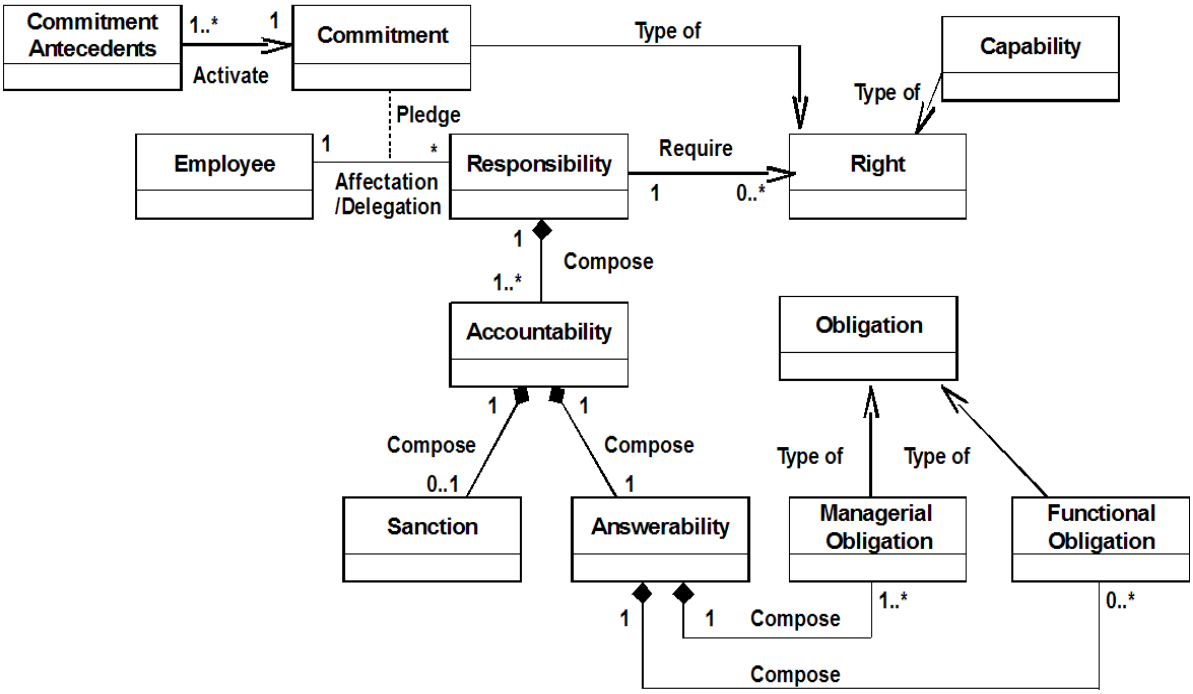

Figure 1. : Responsibility model UML diagram

Accountability is composed of both: answerability and sanction [14] (should it be positive or negative [15]). The answerability is defined in CobiT by the action to report or explain the action or someone else's action to a given authority [3]. This concept needs the existence of an obligation to have a real meaning. An obligation is the most frequently existing concept appearing in all the frameworks. Two main types of obligations exist: functional and managerial obligation. Functional obligation concerns functional actions (direct production of goods) and managerial obligation concerns managerial actions [25].

Right is common but not systematically embedded in the frameworks. It encompasses facilities required by an employee to fulfil his accountabilities. These facilities could include, amongst others capabilities, authorities or the right to delegate.

Capability describes the possession of requisite qualities, skills or resources to perform an action. Capability is a component that is part of all models and methods [4,26,27], and is most frequently declined through definitions of access rights, authorizations or permissions [28,29, 30].

Commitment: the affectation is an activity linking an employee responsible for a specific activity. This employee has to be committed to perform the activity. Although this commitment concept is quite inexistent in IT, it is subjected to many researches in other sciences. As a consequence, we will deepen its explanation in this paper. Issued from sciences like psychology, sociology and management, the commitment remains a virtual concept difficult to define as well as to introduce to a strictly formalized framework. To bypass this difficulty, an alternative solution is the integration, into the standard, of component enforcing the commitment. These components traditionally called "Commitment's antecedent" in literature correspond to real information which can sometimes be implemented and/or managed and which can at least in any case be measurable.

The antecedents may take many forms depending of the type of commitment. These forms are i.e. characteristics and experiences which a person adds to the organization [16], the employee's age and his time with the organization [17] [18] [19], the perception of the job security [20], the culture and style management [21], the employee's investments in time, money and effort [22]. Scientific commitment surveys also highlight that commitment outcomes may really influence the quality and efficiency of the activity achieved. The following list summarizes commitment outcomes:

- The employee's performance [23]. Committed employees perform better because of their high expectations of their performance. Moreover, employees have a high level of performance when they are committed to both their organization and their profession.
- The retention of employees. A lot of study demonstrates the link between the commitment and the employee turnover [22] [23] [24].
- The citizen behavior or extra-role behavior. The research regarding these outcomes remains inconclusive.

Based upon the commitment outcomes and antecedent definition, we may deduce first that being committed to the responsibility of a activity means for an employee an increasing of trust in the accountability attached to the responsibility and more efficiency (and consequently more capabilities) of that employee to perform an action. And secondly, that a certain responsibility (manager) should guarantee a level of antecedents for others responsibility (employee)

4. Analysis of ISO 27001

This section analyzes the responsibility component encompassed in ISO 27001 in order to face challenges highlighted in section 2. The method used is a syntactic reading of the standard to track each references related to the concept of responsibility and assignment of them with the right meaning and right denomination according to our responsibility model.

ISO 27001's main objective is to provide control within a process approach. To achieve that, the standard proposes a PDCA "Plan-Do-Check-Act" model (figure 2) that structures the set of control processes provided in its annex A.

The PDCA encompasses the following four activities:

1. understanding the organization's information security requirements
2. implementing and operating controls to manage the organization's information security risks in the context of the organization's overall business risks;
3. monitoring and reviewing the performance and effectiveness of the ISMS; and
4. continual improvement based on measurement.

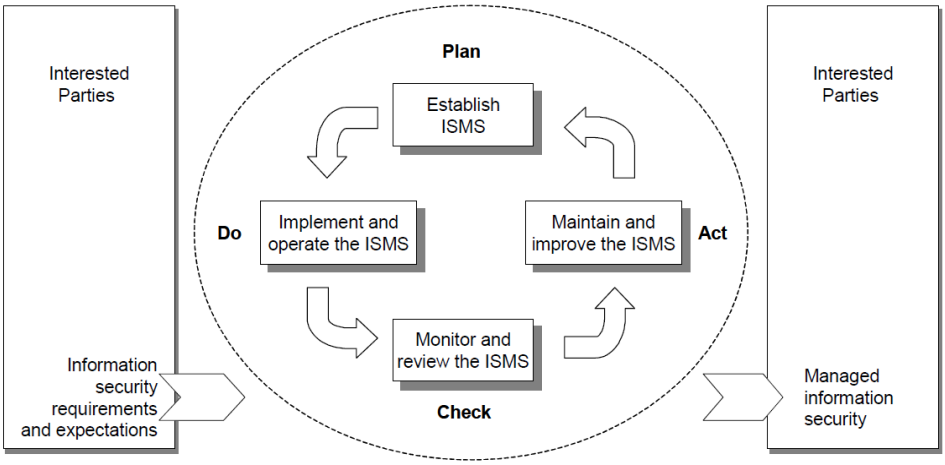

Figure 2. ISO 27001 PDCA model applied to the ISMS

4.1. ISO 27001 Responsibilities

The standard mainly gathers activities to be performed to manage the information security and lists controls necessary to guarantee corporate security objectives. These controls are derived form ISO 27002 and are listed in annex A.

ISMS management activities: Most of the management activities are enumerated in section 4 and are structured following the PDCA framework.

Table 1. : Analyze of the responsibility elements in ISO 27001

Section	Responsibility	Accountability	Right / Capability	Commitment	Stakeholder	Comments
3.4. Information security		X			N/A	ISO 27001 never addresses the accountability as explained in the previous section but it introduces it as an element which defines the information security : *accountability is necessary to trace fraudulent behavior*
4.1. General requirements	X				Organization	The organization shall establish, implement, operate, monitor, reviwe, maintain and improve a documented ISMS
4.2. Establishing and managing the ISMS	X				Organization	Chapter 4.2 lists the main activities for establishing and managing the ISMS. Those activities cover the establishment of policies up to their implementation and control, and finally include corrective actions and prevention tasks. We may rightly assume that some of them are affected to the IT manager and others to the business manager. IT managers responsibilities are i.e. *the implementation of procedures and other controls capable of enabling prompt detection of security events and response to security incidents (4.2.2 h)* and business manager responsibilities are i.e. *Take into account business regulatory (4.2.1. b2), approve the definition of the ISMS (4.2.1 b5) or assess the business impacts upon the organization that might result from security failures (4.2.1 e1)*
4.3 Documentation requirements	X					This section icludes the documentation required for the management of the ISMS. It lists a set of activities to be achieved by the employees responsible for operating tasks related to the ISMS
5.1. Management commitment	X				Management	Section 5.1 *Management commitments* list the main activities under the responsibility of IT and business managers. The standard links the notion of responsibility to the term commitment, but it never refers to the understanding of commitment such as it exists in scientific literature reviewed in chapter 3. Indeed, such as it appears, means that a manager must be committed and consequently, must achieve the task he is responsible for. Although the dual representation of obligation proposed by Dobson [25] is justified to highlight the distinction between operational and managerial function, this representation is not justified to distinguish between the business and the IT manager's accountabilities. Indeed, the repartition of accountabilities between both is uniquely based on the task to be performed rather than on a hierarchical level.
5.2. Provision of resources	X		X		Organization	Section 5.2 *Resource management* lists the resources and competences necessary to manage the ISMS or to perform controles from annex A. According to our model, these resources correspond to the right necessary to be responsible. I.e. the requirement 5.2.2.A): *Determining the necessary competencies for personal performing work affecting the ISMS* , indicates that the standard is sensitive regarding the importance of having the necessary right to assume a responsibility. This chapter however is only summarized in 4 points and consequently, does not help much. The right affectation of resources and competences to stakeholders is under the responsibility of the organization
6. Internal ISMS audits	X				Organization / Management	Section 6 lists the ISMS audits requirements and the responsibilities related to that audit
7. Management review of the ISMS	X		X		Management and interested parties	Section 7 lists the ISMS review requirement and the responsibilities related to that review. One of those requirement concerns the decision of the management regarding the needed resources (7.3.d)
8. ISMS improvement	X				Organization	Section 8 lists the ISMS improvement requirement and the responsibilities related to that improvement

Table 2. : Analyze of the responsibility elements in ISO 27001

Section	Responsibility	Accountability	Right / Capability	Commitment	Stakeholder	Comments
Particular control						
A.6.1.1 Management commitment to information security	X			X	Management	The control A.6.1.1 which argues for clear responsibility assignment and acknowledgement of information security responsibility is a commitment antecedent that is to be provided by the management to the organization
A.6.1.3 Allocation of information security responsibilities				X		That control state that "*All information securities responsibilities shall be clearly defined*". As explained in chapter 3, these elements activates employees and managers commitment
A.8.1.1 Roles and responsibilities				X		That control state that "*Security roles and responsibilities of eployees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy*". As explained in chapter 3, these elements activates employees and managers commitment
A.8.2.2 Information security awareness, education and training			X			That control state that all person involved in control shall receive appropriate training
A.8.2.3 Disciplinary process		X				As Cater [15] explains, sanction is an important element of accountability. ISO 27001 advocates in that control a disciplinary process for employees having committed a security breach

Those activities concern the establishment, the implementation, the monitoring and review, and the maintenance and improvement of the ISMS. The affectation of responsibilities for the achievement of these activities is superficial and incomplete in that only the organization or the management is identified as being responsible.

Controls: Operational controls of ISO 27001 are withdrawn from control objectives listed in ISO/IEC 17799:2005 clauses 5 to 15 and correspond to implementation advice and guidance on best practices.

These controls directly correspond to security practices necessary to be deployed in order to guarantee the corporate information system security. Typical operational controls are *information back-up* (A. 10.5.1), *capacity management* (A. 10.3.1) or *information access restriction* (A. 11.6.1).

The standard has not for duty to fix the responsibilities for each of these controls. However, it appears that one of them (A.6.1.1) advocates that the management is responsible for explicit assignments and acknowledgments of responsibilities related to the controls.

To understand all the responsibility constructs that exist in the standard, we have analyzed it section by section and summarized in table 1 and 2 hereafter.

4.2. Synthesis of ISO 27001 Responsibility

The concept of responsibility exists in the framework, but the elements that compose it are spread from section 3 to section 8 like summarized in Table 1 and in the analyze of the annex A in table 2.

Responsibility: The standard has for objective to provide a framework to manage the security of the information system. As consequence, the responsibilities of the managers are the most detailed. These responsibilities are mainly listed in section 4.2 and 5.1. Section 4.2 gathers the activities to be done by the organization at each of the four steps of the ISMS. Although the employees that are responsible for these activities are not explicitly listed, it appears that both IT and business managers are involved. We make the same conclusions for the section 5.1. In parallel to these 2 sections, the responsibilities of the organization also come along punctually in others sections or controls of annex A. but it is nowhere clearer which precise employee (or role or function) is responsible for which activity or even, which responsibilities have to be taken on by the IT or by the business staff.

In parallel to the activities related to the management of the information security system, the standard enumerates also activities more concerned by the day-to-day operations. These activities are mainly listed in control of the annex A and are i.e.: *all employees […] shall return all of the organization's assets in their possession upon termination of their employment* (A.8.3.2) or *all employees […] shall be required to note and report any observed or suspected security weakness […]* (A.13.1.2). Even there, clear affectation doesn't exist.

Analyzing the responsibility in a deeper way implies to dissociated it, according to the responsibility model, in three points of view: the accountability of the employee, the rights/capabilities required to perform the activity he is responsible for and his commitment to this responsibility.

Accountability: Accountability doesn't exist largely in the standard. This statement is natural in that accountability may only exist when responsibility are clearly defined. As consequence, it is not always clear how an employee is held responsible for the achievement of an activity.

Although the accountability poorly exists, the standard claims for disciplinary process for employees having committed security breach (ctrl A.8.2.3). This control is meaningful but its applicability seems incalculable since the standard doesn't impose answerability.

Right/capability: Rights necessary for assuming responsibility are concisely listed mainly in section 5.2, but without really been a focus of interest or a requirement for the implementation stage. The rights/capabilities listed in this section remain

generic and do not bring any necessary material for using the standard in practice. At the opposite, requesting too much rights or capabilities could lead to an over abundance of them and could lead to a situation of security breach.

Commitment: ISO 27001 deals with the commitment but according to another meaning that the one that the responsibility model stands for. Indeed, the standard uses the word commitment to introduce the management's obligations rather than the manager's personal willingness to achieve an activity.

As we introduce it in the preview section, the employee commitment is an important component of the responsibility and its inclusion in ISO 27001 may bring an important contribution in the responsibility affectation/delegation process. This could be illustrated for instance by the importance for the IT management to delegate responsibility to an employee who strongly believes that the information security is a cornerstone for the corporate development rather than to an employee who considers information security as a cost factor.

Although the commitment appears not to be clearly defined and not to be part of the standard, we observe that some ISO 27001 requirements could correspond to some commitment antecedents. This is for instance the case of antecedents extracted from following controls:

- *role and responsibility are clearly defined* (A.8.1.1);
- *assignment is explicit* (A.6.1.1);
- *management support security with clear direction* (A.6.1.1);
- *Operating procedures shall be documented, maintained, and made available to all users who will require them* (A.10.1.1.).

Whatever the existence of these controls, they're no tailoring or adaptations to the level of responsibility (management or operational) and to the working area of the employee (business or IT). Indeed, the standard does not distinguish between the business management's and the IT management's commitment. However, we may suppose that the antecedents commitment for an IT or a business manager differs. Because an IT manager is naturally more distant to the business goals and values than a business manager, an IT manager could be more interested by side-bets whereas that from a business manager's point of view, the company's goals and values most often direct the choice to apply for a job in a specific company. I.e. a business manager interested in the "health sector" will try to get a job in this field, whereas an IT manager is less involved about the company's finality.

5. ISO 27001 Improvement Perspectives

The above analyzed of ISO 27001 highlights weaknesses at the origin of implementation failures.

The first challenge issued from the survey introduced in section 2 highlights that organizational culture is a strong artifact to be faced when modifying the organizational process. Indeed, management culture and fundamental core business objectives are to be considered as an unavoidable employee's commitment antecedent. The CES survey reports a lack of interest in that matter in most of the companies having replied to the questionnaire. Main reasons for implementing an ISMS are stated most of the time (80%) being certified as a means for gaining competitive advantages on the market and other reasons such as: requests for tenders (28%), legal and regulatory compliance, mandated by customers. Consequently, we argue that to keep employees committed, the reasons for implementing an ISMS should also include a link to the core objective of the company.

The second challenge highlights that the top manager buy-in is a key success factor. Although that this requirement explicitly exists in ISO 27001, CES survey [8] advocates the opposite in practice. Indeed, surveys and use cases show that even if existing at the beginning of the implementation process, the management's commitment tends to disappear afterwards. This result directly affects the time granted by the top manager for the ISMS manager or for the prioritization of activities, i.e. security management activities are abandoned to other types of activities. In this case, the top management's commitment is an accountability linked to its responsibility to promote the implementation of the standard. ISO 27001 does not detail the top management's responsibility but only lists the top management's accountabilities without detailing the necessary rights and commitments.. The top manager responsibility should be better described.

The third challenge is highlighted by 18% of respondents claiming for more time or resources to perform their function. Indeed, looking ahead in the survey shows that only 12% of ISMS manager have the opportunity to be full-time employed in this function which is moreover often cumulated with a Quality Manager position. The employing of external consultants in 54% of the companies is a way of facing the lack of resources but at the same time, is a problem put in exergue by ISMS managers continually trying to solve it. We argue for a better definition of rights and capabilities required to assume the responsibilities at each layer of the organization.

Additionally to these conclusions, it appears that ISO 27001 main objective is to provide an ISMS and as a consequence, all activities at the different security implementation stages are largely discussed. However, even if both responsibility and accountability exist, explicit links between them remains insignificant and kept at the discretion of the manager that is responsible for implementing the standard (mainly requested by controls such as A.6.1.3 *"Allocation of information security responsibilities"*)

6. Conclusion

Ubiquitous Internets claims for more suitable definition of the responsibility of the employees that use the company decentralized IT architecture. Our previous research has provided a responsibility model constructed on inputs from social, psychological and managerial sciences and applied to the IS area.

ISO 27001 is standard that has a paramount significance for the security management of ubiquitous computing. It has a worldwide recognized and aims at directing the implementation of ISMS. However, many surveys and case studies of this implementation argue that some typical challenges, always targeting the same problems, remain unsolved. The objective of this paper is not the improvement of 27001 but to highlight the existence of these challenges and to propose a way to solve them by using an approach centered upon the responsibility model. We propose four points of improvement:

1. To deepen the description of the top management's responsibility;
2. To clearly affect accountability to responsibility.
3. To really take into account employees' commitment. It may be achieved by advocating during the implementation how ISO 27001 will contribute to reach the core objectives of the company;
4. To improve the definition of rights and capabilities needed for each responsibility;

Our future work will focus on the development of tools and methods to sustain the above-listed recommendations. We are currently working with a partner company where all of that tools and methods will be designed and tested.

7. References

[1] ISO/IEC 38500 (2008), International Standard for Corporate Governance of IT (IT Governance)

[2] ITIL (2001), IT Infrastructure Library – Service Delivery, The Stationery Office Edition, ISBN 011 3308930.

[3] CobiT 4.1, Control Objectives for Information and Related Technology, Information Systems Audit and Control Association, www.isaca.org.

[4] Vernadat FB (1995), Enterprise Modelling and Integration, *Chapman & Hall*, London, ISBN 0-412-60550-3

[5] ISO/IEC 15504, "Information Technology – Process assessment", (parts 1-5), 2003-2006

[6] Dulay N, Lupu E, Solman M, Damianou N (2001), A Policy Deployment Model for the Ponder Language , IM'2001, Seattle, IEEE Press.

[7] ISO/IEC 27001:2005, "Information technology – Security techniques – Information security management systems – Requirements", 2005-10-15.

[8] Certification Europe, The Digital Hub, 157 Thomas Street, Dublin 8, Ireland

[9] Feltus C, Petit M (2009). Building a responsibility model using modal logic-towards Accountability, Aapability and Commitment concepts. In *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on* (pp. 386-391). IEEE.

[10] Smith T (2008). Information Security – What's New and What's working, Oceania CACS, Sydney 2008.

[11] Feltus C, Petit M, Ataya G (2008), Definition and Validation of a Business IT Alignment Method for Enterprise Governance Improvement in the Context of Processes Based Organizations, *Corporate Governance of IT International Conference*, Wellington, New Zealand.

[12] Feltus C, Petit M, Vernadat F (2009), Enhancement of CIMOSA with Responsibility Concept to Conform to Principles of Corporate Governance of IT, *13th INCOM IFAC Symposium*, Moscow, Russia

[13] Feltus C, Petit M (2009), Building a Responsibility Model Including Accountability, Capability and Commitment, *ARES 2009*, Fukuoka, Japan.

[14] Jonathan AF (2007), The uncertain relationship between transparency and accountability. *Center for Global, International and Regional Studies*. Reprint Series. Paper CGIRS-Reprint-2007-2.

[15] Stahl BC, Wood C (2006), Forming IT Professionals in the Internet Age: A Critical Case Study, In: Yoong, Pak & Huff, Sid (eds.)*: Managing IT Professionals in the Internet Age*. Idea Group, Hershey, PA: 120 – 139

[16] Mowday RT, Porter LW, Steers RM (1982), Employee-Organization Linkages: The Psychology of Commitment, Absenteeim, and Turnover. New York: Academic Press. *Journal of Occupational Psychology*, 63, pp. 1 – 18.

[17] Buchanana B, II. (194), Building organizational Commitment: The Socialization of Managers in work organizations, *Administrative science Quart.* 19, 533–546.

[18] Hall D (1977), Organizational Identification as a function of Career Pattern and Organizational Type, *Administrative Science Quarterly*, 17, pp. 340 – 350.

[19] Lio K (1995), Professional Orientation and Organizational Commitment among Employees: an Empirical Study of Detention Workers, *Journal of Public Administration Research and Theory*, 5, pp. 231 – 246

[20] Niehoff BP, Enz CA, Grover RA (1990), The Impact of Top-Management Actions on Employee Attitudes and Perceptions, *Group & Organization Studies*, 15, 3.

[21] Florkowski G, Schuster M (1992), Support for Profit Sharing and Organizational Commitment: *A Path Analysis*, *Human Relations*, 45, 5, pp. 507 – 523.

[22] Blau GJ (1985), The measurmement and Prediction of Career Commitment, *Journal of Occupational Psychology*, 58, pp. 277 – 288.

[23] Meyer JP, Allen NJ (1984), Testing the 'Side-Bet Theory' of Organizational Commitment: Some Methodological Considerations, *Journal of Applied Psychology*, 69, pp. 372 – 378

[24] Porter LW, Steers RM, Mowday RT, Boulian PV (1974), Organizational Commitment, Job Satisfaction, and Turnover Among Psychiatric Technicians, *Journal of Applied Psychology*, 59, pp. 603 – 9.

[25] Dobson J, Martin D (2006), "Enterprise Modeling Based on Responsibility", *TRUST IN Technology: A Socio-Technical Perspective*, Clarke, K., Hardstone, G., Rouncefield, M. and Sommerville, I., eds., Springer.

[26] Sommerville I, Lock R, Storer T, Dobson J (2009), Deriving Information Requirements from Responsibility Models, 21st International Conference, CAiSE 2009, Amsterdam, The Netherlands, June 8-12. ISBN 978-3-642-02143-5.

[27] Yu ES, Liu L (2001), Modelling Trust for System Design Using the i* Strategic Actors Framework. Workshop on Deception, Fraud, and Trust in Agent Societies Held During the Autonomous, Eds. Lecture Notes In Computer Science, vol. 2246. Springer-Verlag, London, 175-194.

[28] He Q, Antón AI (2003), A Framework for Privacy-Enhanced Access Control Analysis in Requirements Engineering, REFSQ'03, Austria.

[29] Roeckle H, Schimpf G, Weidinger R (2000), Process-oriented approach for role-finding to implement role-based security administration in a large industrial organization. RBAC '00. ACM, New York, NY, 103-110

[30] Feltus C, Petit M, Sloman M (2010), Enhancement of business it alignment by including responsibility components in RBAC. Business/IT Alignment and Interoperability BUSITAL 2010, 61.

[31] Di Renzo B, Feltus C (2003), Process assessment for use in very small enterprises: the NOEMI assessment methodology, European Software Process Improvement (EUROSPI'2003), Ed. Richard Messnarz, Graz, Austria. ISBN 3-901351-84-1.

[32] Di Renzo B, Feltus C, Prime S (2004), NOEMI, Collaborative management for ICT process improvement in SME: experience report, European Software Process Improvement (EUROSPI'2004), in Norvegian University of Science and Technology (NTNU), Trondheim, Norway. ISSN: 1503-416

[33] Ernst & Young's 2008 Global Information Security Survey, http://www.ey.com/