Definition and Validation of a Business IT Alignment Method for Enterprise Governance Improvement in the Context of Processes Based Organizations

Christophe Feltus, Michaël Petit, Georges Ataya

Definition and Validation of a Business IT Alignment Method for Enterprise Governance Improvement in the Context of Processes Based Organizations

Christophe FELTUS
Center for IT Innovation
Public Research Centre Henri Tudor Luxembourg
christophe.feltus@tudor.lu

Michaël PETIT
Computer Science Department,
University of Namur Belgium
mpe@info.fundp.ac.be

Georges ATAYA
Solvay Business School
Université Libre de Bruxelles Belgium
gataya@ulb.ac.be

Abstract

These days, it is remarkable to note the growing of interest in professional responsibility. Specifically, the responsibility a person commits to when he or she performs a task. Based on a review of research currently performed in the field of policy (from corporate to technical ones), we observe that the perception of responsibility has often been limited to a combination of rights and obligations. In addition, we are seeing a re-emergence in business (for example, in the financial sector) of a belief that business ethics foundation can be improved and that a renewed focus in this area would help to prevent future breakdowns in the system. With regard to improving business/IT alignment and corporate ICT governance, it becomes increasingly important to define a commonly accepted personal responsibility model that embodies important and well-known concepts like accountability, capability and commitment. Moreover, because responsibility constitutes a fundamental notion of management theory, it is likewise identified as a meaningful bridge toward organizational artifacts. Exploiting process-based approach to define policy seems to offer new research opportunities since process-based organization becomes a continuous widely spread structure.

Key Words: ICT Governance, Responsibility model, Capability, Accountability, Commitment.

1. INTRODUCTION

Accounting scandals of 2002 and more recently ongoing market crisis highlight the importance of the Corporate Governance and by consequence: Governance of IT. Following those scandals, a lot of laws and standards were published in order on one hand to guarantee the stability of the financial sector and, by extension, to all sectors of the industrial economy and in the other hand, to enhance the governance all of these public and private companies. Sarbanes-Oxley Act (Sarbanes et al., 2002) Basel II (Basel II, 2006) and EU Directive 95/46 (Directive 95/46/EC, 1995) are some of these laws that aim at providing guarantees over the company's accountability. The ISO/EIC 38500:2008 (ISO/IEC 38500, 2008) is one standard that provides a framework for effective governance of IT. One of the main constraints imposed by these laws and standards is to have responsibilities clearly established and accepted internally by the collaborators and externally by the stakeholders as well. Unfortunately, by depicting the responsibility in a large range of IT oriented frameworks, we come to the conclusion that no global consensus over a responsibility model exists. The scope of our review as targeted organizational models from the realm of IT security, from access control models such as RBAC (Ferraiola et al., 2001), UCON (Park et al., 2002) and OrBAC (Abou El Kalam et al., 2003) up to framework for ICT governance like Cobit and its RACI chart (Cobit 4.1) or the service management like ITIL (ITIL, 2001). We have also investigated the area of requirement engineering, through the analyses of role engineering methods like (Bertino et al., 2005), (Yu et al., 2001), (Antòn, 1996) and (Crook et al., 2002) and through EAM (Enterprise Architecture Model) frameworks like CIMOSA (Vernadat, 2005) or Togaf (Togaf, 2007). The importance of the finding regarding the miss of a common understanding over responsibility has oriented our research and as a consequence, we propose in this paper firstly to introduce our innovative responsibility model that has been elaborated following the review and based on a global comprehension of the concepts. This model has already been largely commented in (Feltus et al., 2007) and (Rifaut et al., 2006). It has been designed to be a structured representation of the responsibility necessary to achieve a finite set of activities (like in a process). The three main components of the responsibility model are Capability, Accountability and Commitment. The capability describes the quality of having the required qualities or resources to achieve a task, the accountability describes the state of being answerable about the achievement of a task, and the commitment is the engagement of a stakeholder to fulfil a task and the assurance he will do it. Hence, the usage of our model is twofold: Firstly, it may be associated with another model and when we use them together, the organizational model is enhanced with responsibility concept and is as a consequence closer to governance requirements (see Fig. 1.)

Fig. 1. Model aggregation

In Fig. 1., Governance requirements are those dictated by newly arising laws and standards like the need for more ethics, more commitment or more accountability. The engineering of these requirements has been performed in (Rifaut et al., 2006). The responsibility model represents the model of responsibility that has been designed based on these requirements. The organizational model is the model to be enhanced with the responsibility components and could be for example the ITIL framework, the CIMOSA framework or a process based enterprise architecture.
Secondly the paper proposes a usage of the model for depicting and enhancing frameworks regarding the definition of policies. This will be illustrated later in the paper with an analysis of a governance principle according to the actors that are responsible for it.
The remainder of the paper is organized as follows: the next section introduces our innovative responsibility model, Section II to IV explain and illustrate how the model may be used in different context. Section II link the responsibility model and the ISO 15504 framework to define policies from the ISO IEC 15504 Framework, Section III links the model and the CIMOSA Enterprise Architecture Model to enhance its elicitation language and finally Section IV explain how the model permits to improve the statement from ISO 38500 that argues, "Director should direct the preparation and use of plans and policies". Moreover, I will illustrate how CobiT and ITIL could provide information to instantiate the model (and by the way, translating the principle in an operational mode).

2. RESPONSIBILITY MODEL

2.1 Components Of The Model

The model of responsibility in Fig. 2 has been initially designed based on an exhaustive review of the scientific literature dealing with that matter and is continuously refined according to newly arising governance requirements. This model is basically designed to be generic enough to be applied to all kinds of organisations, at each abstraction layers and all domains of the organisation. In short, the organisation represents a structure that pursues collective goals. This structure encompasses employees (agent) playing roles and that are responsible to perform processes' activities. In this model, the notion of sequence (the workflow) between the different responsibilities is not represented. Indeed, these transitions are already defined in the other organizational models defining the process model like ISO/IEC 15504.

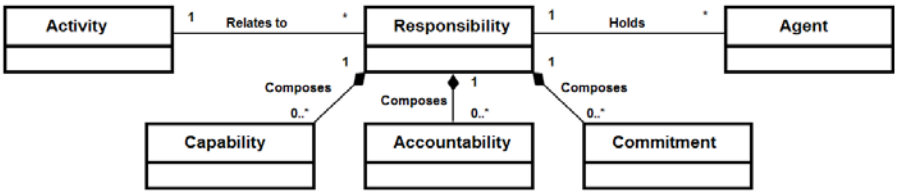

Fig. 2. UML Diagram Responsibility Model

The notion of responsibility is widely used, but no unique definition exists. According to the literature, we may however state that commonly accepted definitions of responsibility encompass the idea of having the obligation to ensure that something happens. Our previous work (Gateau et al., 2008) shows that responsibility can be described as a set of three elements that are Capability, Accountability and Commitment. The relation between responsibility and the three other concepts is of the form 0..* to 1. That means that being responsible involves that the possibility to dispose of many Capacities, Accountabilities and Commitments.

Agent: is a person external or internal to an organization, a system or using a software component. Agent has to achieve the activities he is responsible for. In other models, this concept is also called subject, actor or user. For easing their management, those agents are often grouped together based on their common properties and attributes. As previously explained in the literature overview, the most famous type of classification is based on the concept of role but variations exist such as for example the team, the hierarchy, or some geographical constraints.

Responsibility: It also exists a lot of definitions of responsibility. We may however state that commonly accepted responsibility's definitions encompass the idea of "having the obligation to ensure that something happens". Moreover, the literature review (Feltus, 2008) highlights that being responsible involves that it is possible to dispose of many capacities, accountabilities and commitments. But at the opposite, one commitment and one accountability are linked to one responsibility whether one capability may serve many responsibilities.

Activity: is an operation performed by the agent. Those operations allow him to fulfill its responsibilities This concept doesn't exist in the realm of access control models that describe right or/and obligation needed to perform an operation. E.g.: the right to read a document or the obligation to satisfy conditions before executing an operation. By contrast, "activity" is a main concept in requirement engineering. E.g., in Tropos, a goal may be achieved by fulfilling an activity. The relation between agent, responsibility and activity can be read as: "there is one and only one agent responsible for one activity, and one agent may have many responsibilities and one responsibility may correspond to many activities".

Accountability: is a concept that exists mainly in engineering methods and that appears through the obligation to achieve an activity or to perform an action. This concept describes the state of being answerable about the achievement of an activity. For instance, a strategic accountability for a given responsibility could be: "A project leader must achieve the financial Key Performance Indicators defined for the project". An operational accountability could be: "An IT administrator must give access rights to specific resources of the organisation to members of the project team". Recent laws, like the Public Company Reform and Investor Protection Act of 2002, known under Sarbanes-Oxley and the Basel II requirements for the financial institutions, have put forward the need of more obligation in the hands of agents and more precisely the CEO and CFO. E.g. obligation to be kept informed of whether or not accounts of the enterprise are valid. This accountability is declined under the concept of obligation of result for the operational responsible. ITIL add that only one Agent can be accountable for each task.

Commitment: is the moral engagement of an agent to fulfill an activity and the assurance that he will do it in respect of an ethical code. Commitment is the most infrequent concept. For instance, a strategic commitment for a responsibility could be:" The Chief Financial Officer accepts to manage the accounting department and not commit insider dealing". An operational commitment could be: "An employee of the procurement staff accepts not to use the system for his personal use". Commitment may be declined under different perspectives, such as the willingness of social actors to give their energy and loyalty to social systems or an affective attachment to an organization apart from the purely instrumental worth of the relationship. For James G. March and Johan P. Olsen (March et al., 1995) rules that manage a system exist because they work well and provide better solutions than their alternative. They also observe that peoples' moral commitment is a condition for the existence of a common interpretation of rules. According to that statement and by extrapolating "rules" to stakeholders' capabilities and accountabilities, commitment seems to be an unavoidable component.

Capability: which describes the require qualities skills or resources to perform an activity. Capability is a component that is part of all security models and methods, and is most frequently declined through definitions of access rights, authorizations or permissions.

In the field of access control, traditional policy model such as RBAC do not address this concept. In requirement engineering i* partly introduces it (e.g. when defining dependency as an "agreement" between two agents). Whatever, it is not clear to distinguish if it is a moral concept

or an obligation. For instance, a strategic capability for a given responsibility could be: “A resource must know the strategic objectives of the organisation”. An operational capability could be: “The coach of the resources must have write access to the HR software”.
The consistency between concepts may also be examined based upon the assumption that the capability needed for assuming a responsibility corresponds to the accountability of another responsibility (belonging to another user or role). Both responsibilities’ components capability and accountability are strongly linked to each other (Aubert et al., 2008) An accountability of a role or a person can permit to deduce capability of another role or person and conversely a capability stems from accountability (e.g.: The capability “The coach of the resources must have write access to the HR software” stems from the accountability “An IT administrator must give access rights to specific resources (HR software) of the organization to the coach”).

2.2 Advantages Of The Model

The advantages the responsibility model (Fig. 2) are important for four reasons:

1. It permits to improve the business/IT alignment and brings material to answer to the principle 1 of the ISO/IEC 38500:2008 standard: Establish clearly understood responsibilities for IT.
2. The accountability is bound to the agent rather than to a group of agents (like in others models (Abou El Kalam et al., 2003) This makes the agent personally more involved and more concerned by the activity to achieve because he does not shared the result with anyone.
3. It addresses the commitment aspect of the responsibility and consequently increases the ethics of the business in general.
4. It guarantees that the right capability is affected to the right agent. This advantage guarantees that the agents receive the minimum privileges necessary for achieving their activities and consequently, it decreases the vulnerability of the system.

3. POLICY ELICITATION BASED ON ISO/IEC 15504

That section three focuses on defining responsibility and access control policies from a process based organizational structure. To perform this policy engineering activity, we have oriented our research toward a particular type of company where process-based approaches are in use. Other frameworks also have been chosen such as the matrix approach or the pyramidal one. Future extension of this work could be done for those alternative approaches (Rifaut et al., 2006) Even if process based approaches for formalizing the company’s activity exists for a long time, a number of literature texts and norms deal with it. For example, in (Savén, 2002) Ruth Sara Savén describes a Business Process as a combination of a set of activities within an enterprise with a structure describing their logical order and dependence whose objective is to produce a desired result. In CEN/ENV 12204 (CEN/ENV 12204, 1996) a business process is defined as a partially ordered set of enterprise activities which can be executed to realize a given objective of an enterprise or a part of an enterprise to achieve some desired end-result. Among existing process formalisms, the standard ISO 9000 (ISO 9000, 2005) presents interesting perspectives in that it considers a process as a set of interrelated or interacting activities, which transforms inputs into outputs.

ISO/IEC 15504 (ISO/IEC 15504-1,2 et 5, 2004, 2003 et 2006) confers a structural framework for describing a process and a maturity model to evaluate them. A process, according to ISO/IEC 15504, is described based on the following components:

- Purposes, which describes a process;
- Outcome, which is an observable result of a process. It is an artifact, a significant change

of state or the meeting of specified constraints,

- Base practice, which is an activity that, when consistently performed, contributes to achieving a specific process outcome;
- Work product, which is an artifact associated with the execution of a process. It can be input (required for outcome achievement) or output (result from outcome achievement).

Processes are observable through different outcomes and are achieved by using resources, base practices and work products.

ISO/IEC 15504 does not specifically addresses the responsibility nor the capability and accountability. However, the maturity model that permits to measure the maturity level of the process states that having responsibility defined is needed to be in Level 2,.

Defining policies from business processes are obtained, in our research, by combining responsibility concepts and ISO/IEC 15504 components. We observe quite naturally that first, the Input Work product is a right for a agent to perform an activity; it is by the way combined with the capability. Secondly, the Output Work product is an agent's obligation at the issue of the activity. We combine it with accountability. Fig.2 illustrates that junction of both models. Both responsibilities' components capability and accountability are strongly linked to each other (Aubert et al., 2008) in that accountability of a role or a person permits to deduce capability of another role or person and conversely a capability stems from accountability (e.g.: The capability "An engineer has access to a specific file" stems from the accountability "An engineer has to share a specific file with another engineer").

Fig.3 shows at a more global point of view this conceptual connection between ISO/IEC 15504 component and responsibility concepts.

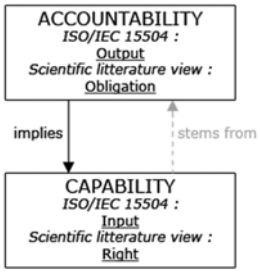

Fig. 3.: Relationship between accountability and capability responsibilities

The possibilities offered by this connection are illustrated with the definition of policies in the field of identity management and access control. Identity management models are composed of responsibilities associated to role, which are given to specific persons. Role should not be confused with the function, for example an engineer (function) can be project manager and developer (roles). However, a person can be linked to one or more roles. The role of a person permits us to define the access policy for that person. For example: to grant access permission to the project management folder on the organization's fileserver. The advantage of that mapping is that it permits to define policies (right and obligation regarding responsibilities) based on the ISO IEC 15504 framework as illustrated in Fig. 4.

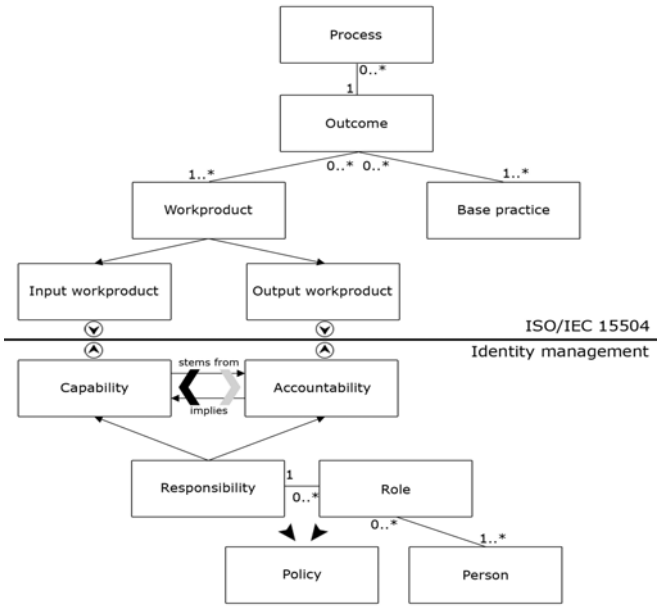

Fig. 4.: ISO/IEC 15504 and Identity management models

4. CIMOSA ENHANCEMENT WITH GOVENRANCE REQUIREMENT

4.1 Analysis Of CIMOSA Basic Responsibility Concepts

The CIMOSA model encompasses (Vernadat, 1995) :

1. A *Modeling Framework* that provides semantic unification of the concepts. It contains three axes (CIMOSA Cube):
   - the GENERATION (with 4 views : Function, Information, Resources and Organization),
   - the INSTANTATION,
   - the DERIVATION.
2. An *Integrating Infrastructure* that supports model execution and acts as a common IT execution platform.
3. The *System Life Cycle* that describes the major phases in the engineering of a CIMOSA system.

The responsibility concepts of our model (section 2) are mainly addressed in the Modeling Framework. By analyzing it, we see that an Agent is a Functional Entity (i.e. an active resource), is represented in the Resource View and appears when resources are derived from the requirements definition to the implementation description. The responsibility is represented in the Organizational View. Indeed, this view is composed with Organization Units that are low level decision centers or work position assigned with responsibilities and authorities, and Organization Cell that are higher level decision centers with a manager, responsibilities and authorities. Those cells are consequently structuring the organizational units into larger entities at different responsibility levels. This information is completed in (Mauchan, 2007) that presents a class diagram of CIMOSA model and highlights how the Organizational Unit is responsible for the process and how this process is composed of activities (or task) that need capability. Additionally to the responsibility element, the CIMOSA Modeling Framework introduces the concept of Authority.

Capability in the current CIMOSA framework is defined as a resource element of the Resource View. This element is linked and needed to the activity concept of the Function View (required capabilities/competencies) and is linked and provided by the agent concept of the Resource View (provided capabilities/competencies). In (Vernadat, 2004) (Kosanke et al., 1999) Capability set is defined as a set of capabilities (i.e. technical characteristics) for technical agents or a set of competencies (i.e. skills) for human agents.

The Commitment is not explicitly taken into account in CIMOSA.

The Accountability of an agent regarding an activity is the obligation to perform that activity and to obtain the expected results. Although both define that activity: the results (control outputs, function outputs and resources outputs) and the agent that perform it (input resource), no explicit link exists between the accountability of that agent and the activity.

Fig. 5 summarizes the CIMOSA's responsibility concepts at a requirement level.

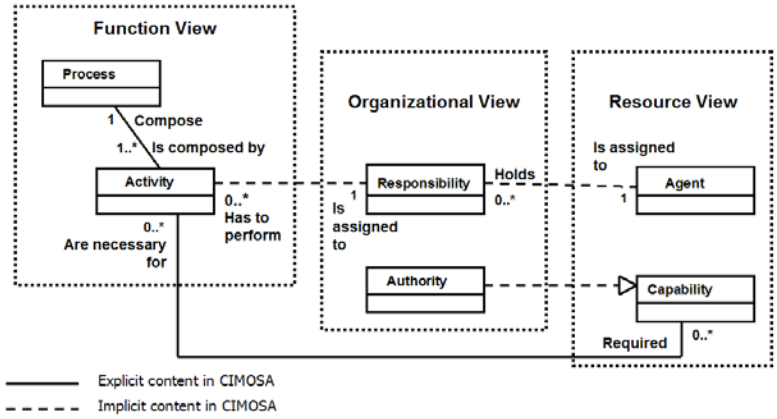

Fig. 5. Basic CIMOSA responsibility model UML Diagram

4.2 Enhancement Of The CIMOSA Framework

The current representation of the responsibility in the CIMOSA model explained in section 4.1 can be improved by incorporating it with our responsibility model presented in section 2. Fig. 2. illustrates that and represents the integration of that concepts at a requirement level:

The *responsibility* concept is explicitly introduced in the Organization view. It is linked to the activity to be performed and to the agent responsible for it. By doing so, we provide the possibility to distinguish the agent that has the required capabilities/competencies to perform the task and the agent that will be accountable of it. This modification will provide facilities to manage the delegation of activities or the possibility to easier replace an agent by another. It introduces as consequence the notion of role (Ferraiolo et al., 2001) in the CIMOSA Framework.

The *capability*, while remaining an element from the Resource View, is no more linked to the activity but it is linked to responsibility. With that modification and in the perspective of being at the requirement level, the agent is responsible if and only if he has the capabilities to perform the activity.

The *commitment* concept will be introduced in the organizational view as a component that compose the responsibility

The *accountability* will exist formally as a component that composes the responsibility. With that concept, it is possible to identify which agent is accountable of which activity.

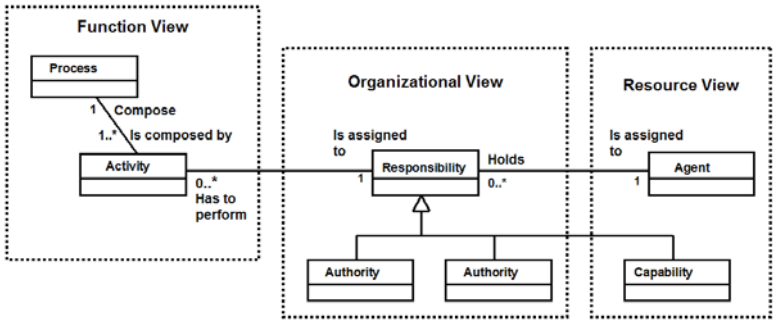

Fig. 6. Improved Responsibility Model UML Diagram

The junction of the CIMOSA model with the Responsibility model is integrated in the CIMOSA language with a new responsibility component that defines the responsibility's elements of the ResourceInput (agent) that perform the activity (Fig. 7)

ResourceInput: *Name of ressource*
Responsibility:
Accoutable : *list of accountabilities*
Capability : *list of capabilities*
Commitment :*list of commitments*

Fig 7. CIMOSA updated language

In parallel to the enhancement of the CIMOSA model, the analysis also permits to understand a new concept: the *Authority*. The Authority will be introduced in the responsibility model as an instance of the Capability. Indeed, the definition of this concept is "the power to command and control others agents". That means, according to our definition of section 2, a well precise type of a right.

5. IMPROVING RESPONSIBILITY IN ISO/IEC 38500:2008

Lot of norms and standards introduce, explicitly or implicitly, responsibility elements. It is the case of standards like ISO 9000, ISO 27000, ISO 14000, and the new standard for ICT governance ISO/IEC 38500:2008. All of theses standards mainly argue that their principles and statements have to be achieved under the responsibility of someone and precise more or less deeply the function or role that has to assume the responsibility. They generally precise what obligations are, but they rarely mention what the awaited commitment is or what the rights accorded to the responsible are.

ISO/IEC 38500 provides limited and synthetic information over its six principle's responsibility. It is justify by the objective of the standard that aims to give guiding principles. However, more information is needed if we want firstly to translate the standard in implementation guides, and secondly if we want that this description of the responsibility answers good governance principles.

According to that analysis, we propose in that last section to explain how the standard is improvable with the responsibility model introduced in section 2. To achieve that, we explain that it based on a requirement extracted form the Principle 2 of ISO/IEC 38500:2008 standard: *Directors should direct the preparation and use of plans and policies that ensure the organization does benefit from the developments in IT*. Based on the description of that requirement in the standard, it is possible to illustrate the responsibility for the activity to be achieved by the *Director* following the structure of the responsibility model. This is illustrated in Fig 8.

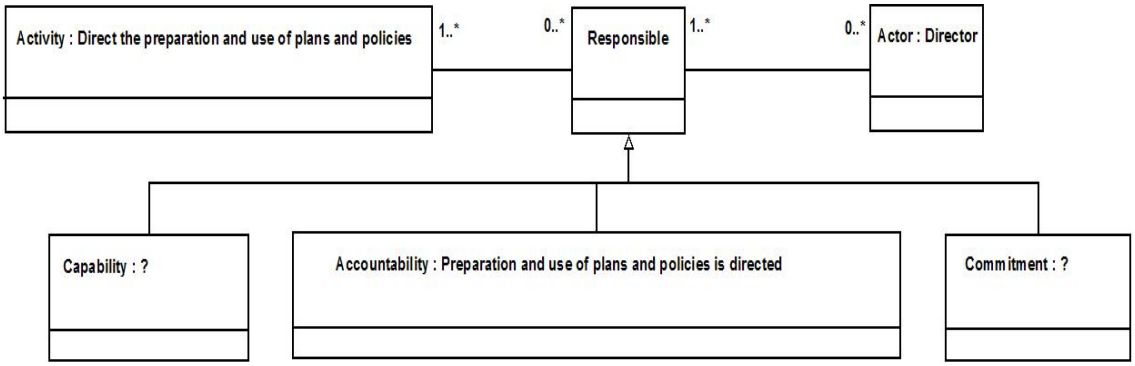

Fig 8: Responsibility in ISO/IEC 38500:2008

When we model the responsibility of the director as illustrated in Fig. 8., it appears that some components of the responsibility (mainly capability and commitment) are not addressed. To complete the missing information, we depict Cobit and ITIL frameworks. Cobit provides more information in its process *PO1, Plan and Organise : Define a Strategic IT Plan* whereas ITIL provides information among others through the *IT Planner role and responsibility.*

It is to note that this paper doesn't provide a finite and rigorous way to define the responsibility but a structuring representation of its component. As consequence, the missing information furnished by Cobit and ITIL is not a unique solution but a portfolio of possibilities to be used to compose the model.

5.1. Instantiation Of The Model According To CobiT Material

The Cobit process that corresponds to that example is the process *PO1, Plan and Organise : Define a Strategic IT Plan.* This process is spited into 5 activities that are : *Link business goals to IT goals, Identify critical dependencies and current performance, Built an IT strategic plan, Built IT tactical plans, analyse programme portfolios and manage project and service portfolios.* Each of these activities owns its own RACI chart and consequently, the statement of the ISO/IEC 38500:2008 framework that affirms that Director is responsible for that activity can be refined when the principle is implemented in the company. To perform that refinement, we consequently need to spit the responsibility of the Director over the set of activities that compose that process. In the case of the activity *Built an IT strategic Plan*, CEO is accountable, CIO is responsible, Business process owner and PMO are consulted and CEO and all others functions are informed. Following CobiT, this activity is achieved by :

- *Engaging with business and senior management in aligning IT strategic planning with current and future business needs*
- *Understanding current IT capabilities*
- *Providing for a prioritization scheme for the business objectives that quantifies the business requirements*

Output of the process is :

- *Strategic IT plan*

This output is, in fact, the accountability of the person that is responsible for it.

Inputs of the process are the following:

- *Cost-benefits reports*
- *Risk assessment*
- *Business strategy and priorities*
- *Report on IT governance status; enterprise strategic direction for IT*

These inputs may correspond to Capabilities needed to perform the task.

Another Cobit Capability is :

- *Understanding current IT capabilities*

5.2 Instantiation Of The Model According To ITIL Material

ITIL also provides information about that activity. By depicting the IT planner role's objectives, it is possible to get more information to instantiate responsibility components of the above model. The IT Planner is responsible for the production and coordination of IT plans. ITIL provides a generic description of the responsibilities that corresponds to 2 generic sub-activities that are "the production of IT plan" and " the coordination of IT plan". The description of that responsibility also encompasses a disparate enumeration of responsibility artifacts. To fulfill our model, we focus our analysis on the sub-responsibility "product IT plan". This sub-responsibility argues that :

The IT Planner is Accountable for :

- *Develop IT plans that meet and continue to meet the IT requirements of the business*
- *Coordinate, measure and review the implementation progress of all IT strategies and plans.*
- *Develop the initial plans for the implementation of authorized new IT services, applications and infrastructure support, identifying budgetary, technical and staffing constraints, and clearly listing costs and expected benefits..*
- *(~~Obtain and~~)*[1] *evaluate proposals from suppliers of equipment, software, transmission services and others services, ensuring that all business and IT requirements are satisfied*

The IT planner is Committed to:

- *Work with senior management and other senior specialists and planners […]*
- *Sponsor and monitor research, development and long term planning for the provision and use of IT architectures, products and services*

The IT planner need following Capabilities :

- *Obtain (~~and evaluate~~) proposals from suppliers of equipment, software, transmission services and others services, ensuring that all business and IT requirements are satisfied*

[1] Some statements of the role and responsibility description fulfill at the same time Accountability and Capability. The unjustified part of the sentence is strikethrough.

The information form CobiT and ITIL is summarized in Fig. 9. In green the information from Cobit and in Blue, the information coming from ITIL.

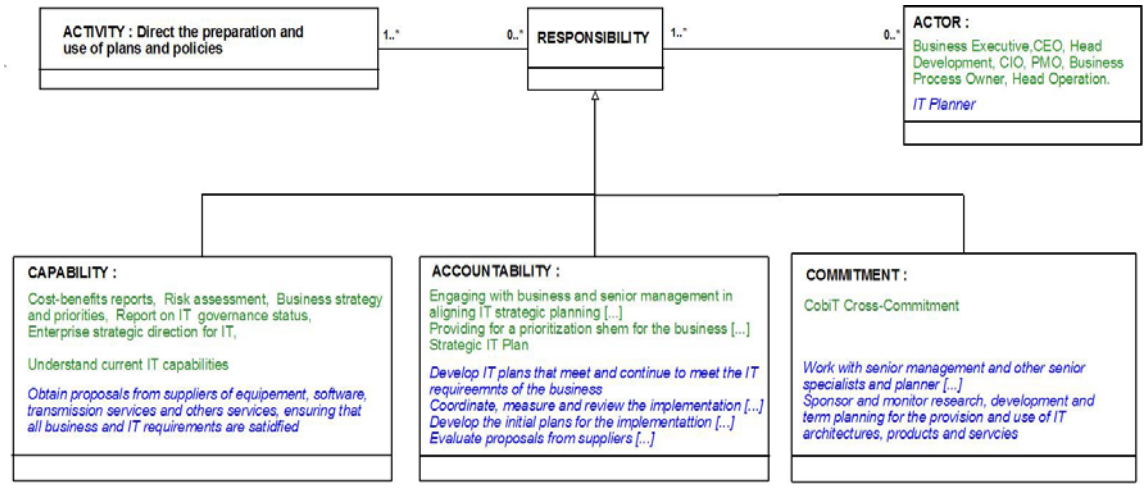

Fig. 9. Instantiated governance principle

Based upon the analysis of CobiT and ITIL, we are consequently able to instantiate one particular principle of ISO/IEC 38500:2008 standard. The responsibility model permit to structure all the components that are requested to design the responsibility according to governance principles whereas Cobit and ITIL permit to provide realistic and pragmatic information to translate that principle in an operational mode.

The model permits also to refine the Cobit process in that it defines more precisely the responsibility for all its the activities. It permits, as consequences, to precise what are the capability, accountability and commitment needed for those activities and not regarding the process in a whole.

The model refines finally the ITIL framework in that it structures in deep its role and responsibility description of functions. For instance, the sentences used to illustrate the responsibility components in section IV.2 are introduced in ITIL without distinguishing upon which activities they are linked (“the production of IT plan” or “ the coordination of IT plan”) and for what purpose they are necessary (for clarifying the obligation and the commitment necessary for the responsibility or for refining its needed capability).

6. CONCLUSION

Current economic context advocates for a deeper and more global adoption of the governance of ICT principle. One of those principles is to have responsibility clearly defined and aligned with the business goals.
The analysis of the literature in the field of IT security, requirement engineering, or enterprise architecture modelling has permitted to define an innovative responsibility model. This model is very simple and generic enough to offer the possibility of being used for a large range of activities. It is constructed upon the concepts of Capability, Accountability and Commitment.
This paper presents three possibilities of using the model:

- The first exploitation of the model is for the creation of policies (business, IT or security). This exploitation is made possible by joining the model with the ISO/IEC 15504 standard and by mapping responsibility component and element of the process framework.
- The second exploitation is the enhancement of the CIMOSA enterprise architecture model with a more structured representation of the responsibility. The junction of the responsibility model and the CIMOSA framework leads to an enhancement of the CIMOSA language that directs the instantiation of all IT components.
- The third exploitation is the extension of the description of responsibility in corporate governance principles. This deeper description permits to bring a first contribution to the translation of corporate governance principles to an implementation guide of those principles

7. REFERENCES

Abou El Kalam, A., El Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miège, A., Saurel, C., Trouessin, G. (2003), Organization-Based Access Control, IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy'03), 4-6 juin 2003, Côme, Italie, pp 120-131.

Antón, A. (1996), *Goal-Based Requirements Analysis*. Second ICRE'96, Colorado Springs, USA.

Aubert, J., Gateau, B., Incoul, C., Feltus, C. (2008), *SIM : An Innovative Business-Oriented Approach for a Distributed Access Management*, International Conference on Information & Communication Technologies: from Theory to Applications (IEEE ICTTA2008), Damascus, Syria.

Basel II (2006), Bank for International Settlements BIS: International Convergence of Capital Measurement and Capital Standards: Revised Framework – Comprehensive Version.

Bertino, E., Mileo, A., and Provetti, A. 2005. *PDL with Preferences*. IEEE international Workshop on Policies For Distributed Systems and Networks, Policy 2005 – Vol. 00, IEEE Computer Society, Washington, DC, 213-222.

CEN/ENV 12204 (1996): Advanced manufacturing technology – Systems architecture - Constructs for enterprise modelling, CEN TC 310/WG1.

CobiT 4.1, *Control Objectives for Information and Related Technology*, Information Systems Audit and Control Association, http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

Crook, R., Ince, D., Nuseibeh, B., (2002) *Towards an Analytical Role Modelling Framework for Security Requirements*, Security Requirements Group, Departement of Computing, The Open University, Walton Hall, Milton Keynes, MK7 6AA, UK.

Directive 95/46/EC (1995), European Union: Directive 95/46/EC of the European Parliament and of the Council. Official Journal of the European Communities, pp. 28-31.

Feltus, C. and Rifaut, A. (2007), *An Ontology for Requirements Analysis of Managers' Policies in Financial Institutions*, I-ESA2007, Madeira, Portugal.

Feltus, C. (2008), *Preliminary Literature Review of Policy Engineering Methods - Toward Responsibility Concept*, ICTTA2008, Damascus, Syria.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., D. Kuhn, R., Chandramouli, R. (2001), Proposed NIST Standard for Role-Based Access Control, *ACM Transactions on Information and System Security*, 4 (3), 224-274.

Gateau, B., Feltus, C., Aubert J., Incoul, C. (2008), *An Agent-based Framework for Identity Management: The Unsuspected Relation with ISO/IEC 15504*, RCIS 2008, Morocco.

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

ISO 9000:2005 (2005), Quality management systems - Fundamentals and vocabulary.

ISO/IEC 15504-1 (2004): Information technology - Process assessment - Part 1: Concepts and vocabulary.

ISO/IEC 15504-2 (2003): Information technology - Process assessment - Part 2: Performing an assessment.

ISO/IEC 15504-5 (2006): Information technology - Software Process Assessment - Part 5: An exemplar process assessment model.

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

Kosanke, K., Vernadat, F.B. and Zelm, M. (1999) *CIMOSA: enterprise engineering and integration Computers in Industry*, Volume 40, Issues 2-3, Pages 83-97.

March, J. G. and Olsen, J. P. (1995) *Democratic Governance*, New York, The Free Press, 1995, 292 pp.

Mauchan, M. (2007), thèse « *Modélisation pour la simulation de chaines de production de valeur en entreprise industrielle comme outil d'aide à la décision en phase de conception / Industrialisation* »

Park, J., Sandhu, R., (2002) Originator Control in Usage Control, *Policy 2002*, Monterey, California, U.S.A.

Rifaut, A. and Feltus, C. (2006), *Improving Operational Risk Management Systems by Formalizing the Basel II Regulation with Goal Models and the ISO/IEC 15504 Approach*, REMO2V'2006, Luxembourg

Sarbanes, P. S. and Oxley, M. (2002) "*Sarbanes-Oxley Act of 2002*".

Savén, R. S. (2002), *Process modelling for enterprise integration: review and framework*, 13th International Working Seminar on Production Economics, Igls/Innsbruck, Austria, February 18-22.

Togaf (2007), *The Open Group Architecture Framework* (TOGAF 8.1.1 'The Book'), 2007 Edition , Van Haren Publishing

Vernadat F. B. (1995), *Enterprise Modelling and Integration*, Chapman & Hall, London , ISBN 0-412-60550-3

Vernadat, F.B. (2004), *Enterprise Modelling: Objectives, constructs & ontologies*, Tutorail EMOI-CaiSE Workshop, Latvia.

Yu, E. S. and 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