Requirements Engineering for Improving Business/IT Alignment in Security Risk Management Methods

N. Mayer[1, 2], E. Dubois[1] and A. Rifaut[1]
[1] Public Research Centre Henri Tudor, 29, av. J. F.Kennedy, L-1855 Luxembourg, Kirchberg
eric.dubois@tudor.lu, andre.rifaut@tudor.lu
[2] University of Namur - Computer Science Department rue Grandgagnage, 21, B-5000 Namur, Belgique
nicolas.mayer@tudor.lu

Abstract: Information systems (IS) security within organizations is more and more focused around risk management approaches. Central to these approaches is the need for a better understanding of the required alignment between the business view of the organization and the architecture of its underlying IS. Through the use of requirements engineering techniques, the paper suggests how this business/IT interoperability issue is tackled together with the clarification of the underlying security risk management ontology.

Keywords: risk management, security, requirements engineering, business/IT alignment, ontology

1. Introduction

For the last twenty years, security concerns have increasingly impacted the development and the exploitation of Information Systems (IS), both in public and private organizations. The pressure is still increasing in many sectors and organizations, where specific directives impose advanced security Risk Management (RM) practices. In this context our contribution is mainly concerned with a better handling of security in IS, through an improved RM approach, based on a better understanding of the required interoperability needed between the business of the enterprise and the architecture of its underlying IS. More precisely, we argue how recent advances in Requirements Engineering (RE) methods and modeling techniques can help in a more systematic alignment between business and IT. We also illustrate how the elaboration of an ontology helps understanding the RM domain.

In this paper our aim is to demonstrate this added value through the handling of a case study, considered as a benchmark for a traditional RM method [2]. We propose the use of the *i** language [7] to illustrate the complementary nature and the possible integration of RE modelling approaches with traditional security RM approaches. In Section 2 we review the key concepts of security RM methods.

Section 3 suggests how RE can help in achieving a better understanding of the business assets and the identification of their associated security goals. In Section 4 we take profit of RE to identify security requirements in a more systematic way and at different abstraction levels. Finally, Section 5 explains the alignment between the business and its underlying IS through a risk-based security reasoning, where different architectural solutions need to be evaluated against the identified security goals and requirements.

2. Security risk management concepts

Today a number of commercial methods (like OCTAVE, ITBPM, CRAMM, MEHARI, EBIOS, etc. [10]) are made available to IT security officers in organizations, for performing a risk analysis of security problems and identifying security solutions that are the most adequate.

The main objective of all these approaches is to guarantee some specific form of business/IT alignment, accrediting that the right level of security solution is put in place, with respect to the value of the assets of the organization to be protected. The key ingredients of a successful business/IT alignment in terms of security management are:

- *Business Assets* are anything that has economic value to the organization and that is central in the realization of its business objectives. The protection of these assets is essential for the survival of the organization.
- Within organizations, business assets management relies heavily on IS. *IS Assets* (including IT resources) are any components that are part of IS and of their operating environment. They are supporting business assets.
- *Security* is the main focus of the IS for the scope of this paper. It defines different qualities expected from the IS. Besides the pure security aspects (like confidentiality of data), it is also related to aspects like safety, reliability, etc.
- *Risk analysis* is the essential equation to be kept in mind when handling the different security qualities. For each IS asset, one has to ask questions about its vulnerabilities, the existence of potential threats capable of exploiting these vulnerabilities and the impacts of this exploitation on the running business. All this risk analysis activity results in the identification of best controls (security risk treatment) to be implemented.

The ontology of concepts introduced above is summarized in terms of the UML-like class diagram presented in Figure 1.

Using traditional security RM methods shows a number of weaknesses. They are first related to the lack of formality in the documents produced. Moreover, there is an absence of methodological guidance regarding the introduction of RM activities into system engineering, or regarding the identification of assets and security goals within RM methods. To overcome these problems, in the rest of the paper, we illustrate the benefit of the integration of RE techniques and concepts in security RM. Regarding the modelling language, we use *i** [7] that has been found appropriate in terms of an integrated framework supporting the different concepts that are needed, ranging from early business modelling to an architecture

description. Nevertheless other RE formalisms could also be used with the proposed approach.

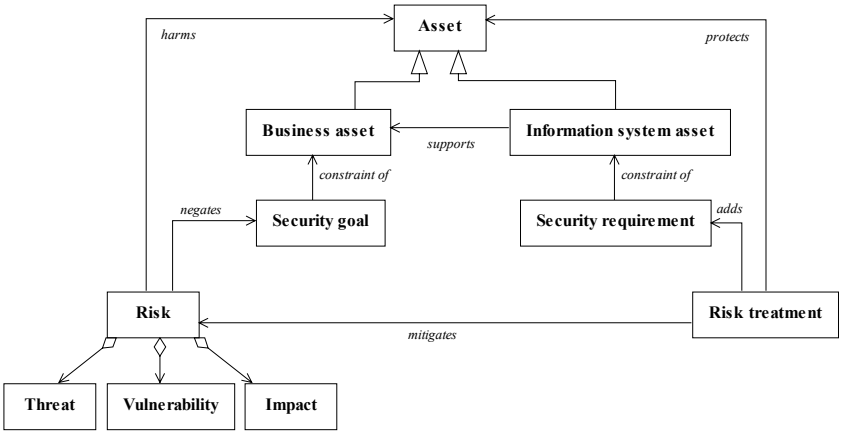

Fig. 1. Security risk management model

3. Identification of business assets and of their associated security goals

The proposed approach is actually validated through the handling of several case studies. For the purpose of this paper, we propose to consider the case of a SME active as an architecture consulting firm in the building domain. In particular, its expertise is in the production of construction plans for factories and buildings. The case study is used as a benchmark for a RM method and is extensively discussed in [2]. The different activities run by the consulting firm can be introduced through an *i** diagram (Figure 2) where we can read that:

- The company is made from different departments (Study office, Administration, Sales department), the last two of them being in relation with external Clients. All these entities are represented in terms of the *i* actor* concept.
- These actors have dependencies between them. A first type of dependency is *goal* dependency. Three goal dependencies are represented in Figure 2:
  - Manage accounting
  - Manage disputed legal claims and technical litigation
  - Manage projects
- A *task* dependency is used when an actor should perform an activity. In our case, Study office does "Structure calculation" for the Sales department.
- Actors are also dependent on *resources* to provide. Study office should provide "Technical plans" and "Models" to Sales department and Sales department should provide "Estimates" to their Clients.

- The last type of dependency is the *softgoal* dependency. It differs from the goal dependency because a softgoal does not have clear-cut criteria of satisfaction. Its illustration will appear later.

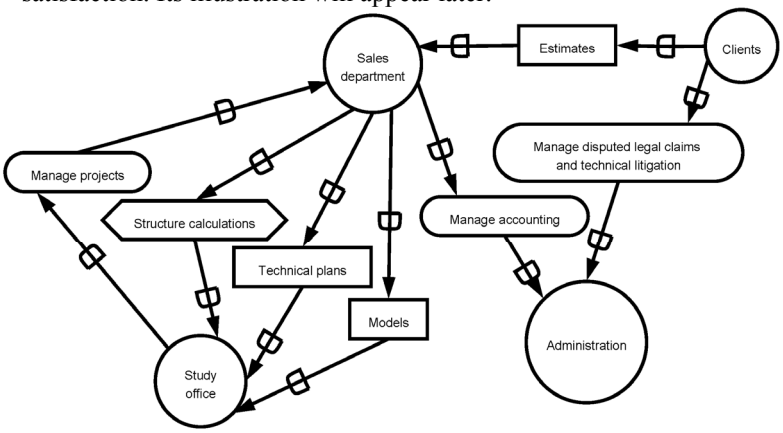

Fig. 2. Consulting firm business model

3.1 Business value analysis

The first security RM activity is associated with the identification of the business assets. The identification of these assets can be improved by the understanding of the economic value associated with them. In the RE and business modelling community, there is a growing concern regarding the development of business value ontologies [13,14], as well as their enactment through business models, where are considered economic actors, economic relationships, and value objects exchanged [15,16]. In [17], a link is established between the e3-value model and *i**. In line with these approaches, our proposal for the identification of business assets relies upon the analysis of the *i** model and, more particularly, of the nature of the dependency. For example, a dependency could be related to some information that has some economic value or to the execution of a process that is critical within the value chain of an organization. The number of dependencies and the significance of them (which cannot be shown in an *i** model) can help in assessing the criticality of a business asset on the basis of its economic value.

In *i** terms, the analysis of dependencies results in the identification of business assets that are associated with a goal to be achieved, a task associated with a way of doing it and a resource associated with a physical or an informational entity. In our case study, from the analysis of Figure 2, one can for example concludes that a number of information like "Estimates" and "Models" are business assets as well as the "Structural Calculation" task, which is associated with the key know-how of the company.

3.2 Derivation of security goals

Once the business assets are identified, the security RM methods propose to elicit security objectives concerning these business assets. Different taxonomies of objectives are proposed by those methods. The most classical one is Confidentiality, Integrity and Availability defined as [3]:

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

As already demonstrated by multiple authors [6,7,19] security objectives can be easily mapped into RE goals, with the benefit of achieving a better structuring and supporting of a (possibly formal) reasoning. Figure 3 shows an excerpt of the goal tree that is elaborated in the context of our case study. Its elaboration results from a two-steps iterative process:

1. Application of the security goal taxonomy to the different identified business assets. For example, the "Confidentiality" (generic goal) of "Estimates" (business asset) is considered as a security goal.
2. Structuring the identified goals with a hierarchy that indicates the significance of the different goals and their contribution to higher level goals that can either be part of the company strategy or related to external factors (like e.g. the trust of customers or the enforcement of legal obligations).

For example, in Figure 3, one can read that the "Confidentiality of Estimates" goal directly contributes to "Customer confidence", which do not want that some important information are disclosed to competitors. Note that additional quantitative or qualitative information about the significance of goals could be added to the goal tree like those proposed in [18].

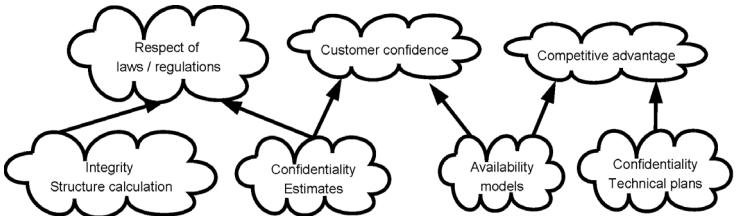

Fig. 3. Security goals

Security goals conform to the definition of softgoals in *i** [9] and Figure 4 depicts the identified terminal goals (leaves of the goal tree). In some cases, analogously to the proposal of [19], they can also be represented as security dependencies, where the position of the security softgoal indicates the actor who has to satisfy it. With respect to the initial business model presented in Figure 2, one can notice the

introduction of a new actor: the "Regulatory Authority". These additional actors correspond to additional identified stakeholders having security concerns.

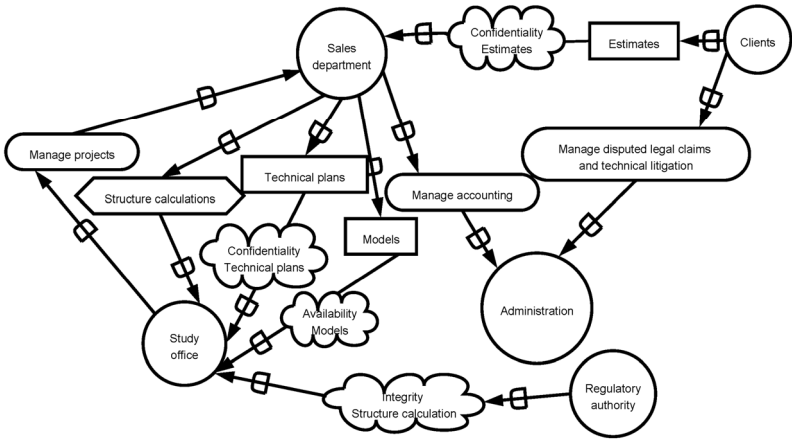

Fig. 4. Actors diagram

4. Identification of high-level requirements

In the previous section we have shown how security objectives in classical RM methods can be mapped in terms of RE business goals. In this section we explain how these goals can be incrementally refined in terms of requirements on the software system.

4.1 From goals to requirements

The discussion started above is summarized in terms of enhancements brought to the initial security RM model presented in Figure 1. Figure 5 zooms on some ontological extensions that are related to the concepts of assets, security goal and security requirement. On the left part of Figure 5, one can read the introduction of the security goals taxonomy introduced in the previous section.

The second extension presented in Figure 5 is related to the concept of constraint. As pointed in the work of Lin *et al.* [5] or Moffet *et al.* [1], there is a need to map goals expressed at the business domain level, in terms of security properties expressed at the IS domain level. For example, a "Confidentiality of Patient Information" goal can be mapped into an "Unauthorized access to Patient Record" constraint. At this stage, it is important to recall that the IS is still seen as a black box, offering a set of services (like e.g. "Manage accounting") without any details about how they are implemented in terms of an underlying IS infrastructure. As also shown in problem frames research literature [1,5], this intermediate level of requirements is of an utmost importance for being able to reason over the properties of a system, in terms of its external behavior expected from its users. With respect to existing RM methods, the concept of constraint presents an

important benefit of being able to reason at a more abstract level, with also the benefit of revisiting alternative design decisions for future evolutions of the system. When expressing an "Unauthorized access" constraint on the IS, there is no further idea about the operationalization of this constraint, which can be later implemented either through a web access portal and/or through the presence of a physical security agent in the building. In Figure 5, we show an excerpt of the taxonomy of constraints. Due to the lack of space, this taxonomy is not completely presented.

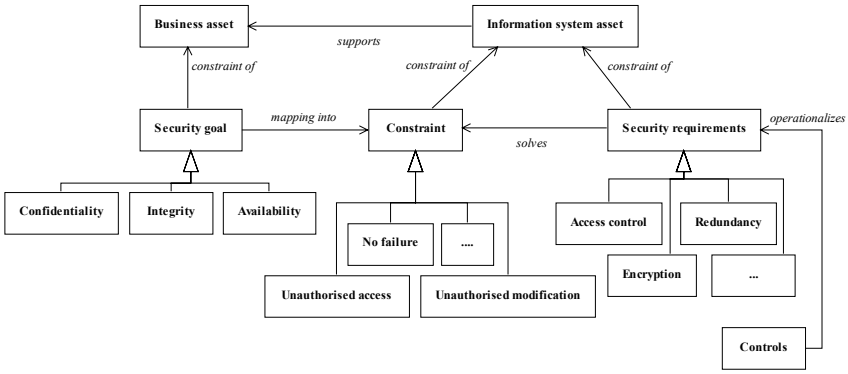

Fig. 5. Focus on the requirements part of the security risk management model

Finally, on the right part of Figure 5, one can see another partial taxonomy associated with security requirements. Most of the RM methods introduce such requirements and make available knowledge bases associated with them. Still the concept of "requirement" can have different meanings in different methods. In some cases, these security requirements are technical requirements associated with properties attached to different types of components found in the IS infrastructure: software components, database components, hardware components, network components, etc. In some other taxonomies, security requirements correspond to more generic Non-Functional Requirements (NFR) [9] attached with guidelines that can later help the architect during its design. In the Common Criteria [4], we found examples of the two types of requirements. Some are generic ones like "the necessity to put in place some access control mechanism" (but no details about how to implement them are given) while some are more technical requirements like those related to "the length of the key to be used in an encryption mechanism". From a methodological point of view, it is important to make a distinction between both of them. In particular, at this analysis stage, only the non-technical ones are relevant. Note also the link between a security requirement and a constraint. A constraint describes the security problem to be solved, while the security requirements give some elements regarding the solution to be put in place.

4.2 Identification of constraints and security requirements

In the context of our case study, at the late RE stage, the IS is introduced. The resulting model is presented in Figure 6, where is detailed the "Study Office" actor, as well as its interactions with the "ePlan" software system. "ePlan" offers collaborative support for a set of services used by the different departments of the consultancy firm and, particularly, around the "Structure calculations" activity.
The initial "Structure calculations" task dependency, identified at the business level between "Sales department" and "Study office", is now refined at the IS level, where it can be read that two agents are performing this task. A "Junior study officer" is using an "ePlan" structure calculation service on the basis of a "Technical dossier". Then, for authorizing structure calculations to be transmitted to "Sales department", a "Senior study officer" validates the results produced by the calculation tool. After the validation, she/he notifies that calculation is complete, using the notification "ePlan" service, to the "Sales department".

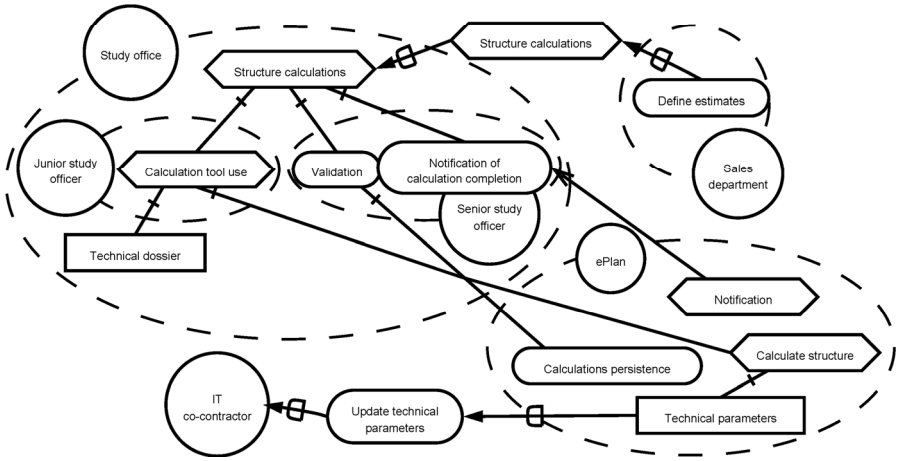

Fig. 6. Introduction of the IS

In this model, there is also a new actor introduced: an "IT co-contractor", expert in structure calculation tools, is in charge of periodically updating "Technical parameters" of the "ePlan" calculation service, according to changes occurring in the regulations or in the materials that are used.

At the level of this IS model, we can then express how security goals described at the business level are transformed into constraints at the IS level. Hereafter, as an example, we consider the "Integrity Structure Calculation" softgoal elicited in Figure 3 and 4.

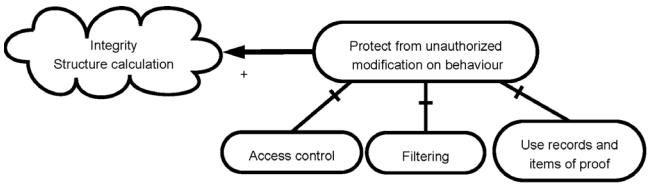

Fig. 7. Constraints and requirements elicitation

In Figure 7, one can read that the goal is mapped in the "Protect from unauthorized modification on behaviour" constraint. This constraint can be systematically derived from the fact that "Structure Calculation" is an IS asset with a behavioral (opposed to structural, like data) type, for which unauthorized modifications of the behavior have to be prevented. Associated to our model presented on Figure 6, we have also patterns for decomposing constraints into security requirements. In this case, the application of a pattern results in the introduction of three security requirements, which contribute to the resolution of the constraint:

- Access control: a preventive measure on an internal component controlling access and modification
- Filtering: a preventive measure acting on external elements for controlling access of them to a system
- Use records and items of proof: a detective measure acting as a log on a system component

These three requirements can be used together (as suggested in the case study of [2]) or alone. Moreover, they not only answer to the proposed constraint, but, in other situations, they can be requirements contributing to solve other constraints.

5. Risk Analysis at the Architectural stage

The next activity is related to the architectural phase of the IS. This is at this stage that the different components of the architecture are incrementally identified and that we need to discover controls, i.e. the counter-measures that can be used for fulfilling security requirements (see right part of Figure 5). Identifying the most adequate one is central to the process of security risk treatment.

Back to our running example we are now handling the specific "Use records and items of proof" security requirement identified at the end of Section 4.2. If we consult lists of controls attached with this requirement in the RM methods knowledge bases [2], different solutions can be found. For example, in Figure 8, we can read that the requirement can be met with a solution based on "Video-surveillance" as well as with IT-based solutions deployed at network, hardware or software levels.

Each control can be further described. For example, in Figure 8, we can read that "Software Logging" control is made of three tasks, extracted from the case study example [2]:

- Structure Calculation tool should be audited

- Rules should be defined to analyze audited event according to potential security violation
- Trace data analysis tool should be available to analyze audited event

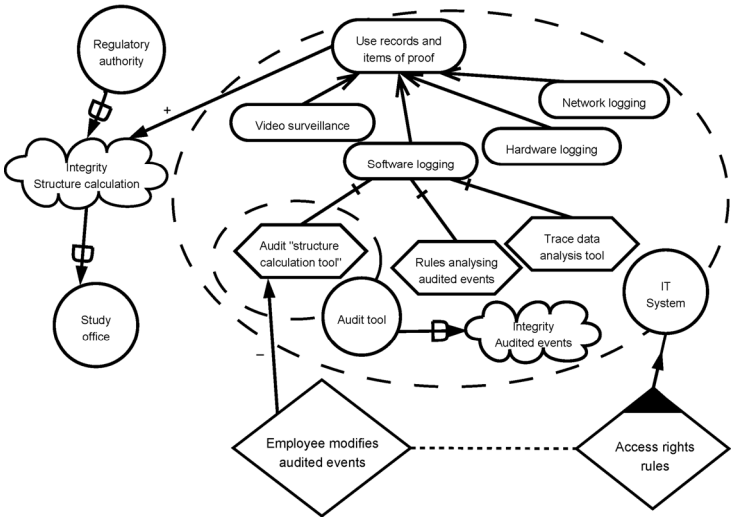

Fig. 8. Risk analysis and controls

Each control has a cost in terms of required development, deployment, exploitation and maintenance activities. Therefore the selection of the most appropriate control is the result of a complete cost-benefit analysis (like in [11]) complemented with a risk analysis based on available information and statistical data related to vulnerabilities, threats and impacts. In our example, this analysis can result in the identification of a threat associated with an internal employee that could modify audited events. This threat is also related to a potential vulnerability identified as the consequence of a bad definition of access right rules (another example of vulnerability could be related to problems in the physical access to the server room). This information is represented in Figure 8 through some *i** notational extensions (diamond with white and black corners). Those notations are inspired from some of our preliminary work reported in [8,10,12].

The final design decision for installing or not the software logging solution will result from the balance established between the cost of the solution, the impact of the occurrence of the risk on the business and the risk potentiality. In our example, we will consider that the "Software logging" control is well suited considering the cost of the solution and the results of the risk analysis. Then, some new security goals for reducing this risk need to be proposed. In our case, it is concerned with a goal of "Integrity Audited events" shown in Figure 8. With the emergence of this new goal, the constraints elicitation (like in Figure 7) needs to be applied again for eliciting a security solution to this security flaw. The method should thus be used in an iterative and incremental way.

6. Conclusion

In this paper we suggest how state-of-art security RM, based on business/IT alignment, can be enriched with recent RE research results regarding security concerns. The alignment between RM and RE methods is proposed on the basis of a meta-model associated with an integrated RM and security ontology. Our approach is extending the work of Moffett *et al.* on the Security Requirements Framework [1]. Besides the concepts of threats on assets, our proposed ontology integrates all the RM concepts like threat, vulnerability or impact. This integration is also reinforced by the proposal of some methodological guidelines regarding the reconciliation of a RE top-down process with a RM process usually applied in a bottom-up way. Our work takes profit of a number of results published on security and RE topics. Of a particular interest is the work of Mouratidis *et al.* [19], which also propose an incremental elaboration of security requirements from an early to a late RE stage, including their handling at the architectural level. This work also introduces interesting *i** extensions with an associated Tropos formalization. Our future plans are related to:

- The development of a toolset supporting the proposed approach. The kernel will be a repository based on the RM model presented all along this paper.
- The investigation of an adequate RM component, central in the toolset, and offering a set of advanced features like those developed by Feather [11] in support to the design and development of complex systems.

7. Acknowledgement

The work is partially supported by the LIASIT (Luxembourg International Advanced Studies in Information Technologies) Institute. It also takes profit of the participation of the authors to the TG5 and TG7 groups of the INTEROP Network of Excellence.

8. References

[1] J.D. Moffett, C.B. Haley, and B. Nuseibeh, "Core Security Requirements Artefacts", *Technical Report Number 2004/23*, Department of Computing, Open University, UK, 2004.

[2] Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) (2004, February), Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS), from http://www.ssi.gouv.fr/fr/confiance/ebios.html

[3] ISO/IEC 17799:2005, Information Technology – Security techniques - Code of Practice for Information Security Management, Geneva, 2005.

[4] Common Criteria for Information Technology Security Evaluation, Version 2.2 (2004), ISO 15408, from http://www.commoncriteriaportal.org

[5] L. Lin, B. Nuseibeh, D. Ince, and M. Jackson, " Using Abuse Frames to Bound the Scope of Security Problems ", *Proceedings of the 12th IEEE International Requirements Engineering Conference*, IEEE Computer Society Press, Kyoto, Japan, 2004.

[6] A. van Lamsweerde, and E. Letier, "Handling Obstacles in Goal-Oriented Requirements Engineering", *IEEE Transactions on Software Engineering, Special Issue on Exception Handling,* Vol. 26 No. 10, October 2000.

[7] L. Liu, E. Yu and J. Mylopoulos, "Security and Privacy Requirements Analysis within a Social Setting", *International Conference on Requirements Engineering (RE'03)*, Monterey, California, September 2003.

[8] P. Gaunard, and E. Dubois, "Using Requirements Engineering Techniques for Bridging the Gap Between Risk Analysis and Security Policies", *18th IFIP International Information Security Conference*, Athens, Greece, May 2003.

[9] L. Chung, B.A. Nixon, E.Yu, J. Mylopoulos, *Non-Functional Requirements in Software Engineering*, Kluwer Academic Publishers, Boston, 2000.

[10] E. Dubois, N. Mayer, A. Rifaut, and V. Rosener, "Contributions méthodologiques pour l'amélioration de l'analyse des risques", *Les enjeux de la sécurité multimédia Vol.1 (traité IC2, série informatique et SI)*, Hermes, 2005. ISBN : 2-7462-1207-2

[11] D.P. Gilliam, and M.S. Feather, "Security Engineering: Systems Engineering of Security through the Adaptation and Application of Risk Management", *INCOSE 2004 - 14th Annual International Symposium Proceedings*, Toulouse, France, Jun 20-24 2004.

[12] N. Mayer, A. Rifaut, and E. Dubois, "Towards a Risk-Based Security Requirements Engineering Framework", *11th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'05)*, in conjunction with CAiSE'05, Porto, Portugal, June 2005.

[13] A. Osterwalder, and Y. Pigneur, "An ontology for e-business models", *Value Creation from E-Business Models*, W. Currie, Butterworth-Heinemann, 2004.

[14] M. Schmitt, B. Grégoire, S. Ramel, C. Incoul, P. Brimont, and E. Dubois. "If business models could speak! Efficient: a framework for appraisal, design and simulation of electronic business transactions", *International Conference on Enterprise Integration and Modelling Technology (ICEIMT'04)*, Toronto, October 2004.

[15] J. Gordijn, V. Kartseva, J. Schildwacht, R.J. Wieringa and J.M. Akkermans, "Developing a Domain-Specific Cross-Organizational RE Method", *Proceedings of the 12th IEEE International Requirements Engineering Conference*, M. Aoyama, Motoshi Saeki, Neil Maiden (eds), IEEE CS, Kyoto, Japan, 2004.

[16] M. Lankhorst. et al., *Enterprise Architecture at Work – Modelling, Communication and Analysis*, Springer-Verlag, 2005. ISBN: 3-540-24371-2

[17] B. van der Raadt, J. Gordijn, and E. Yu, "Exploring Web Services Ideas from a Business Value Perspective", *Proceedings of the 2005 13th IEEE International Conference on Requirements Engineering (RE'05)*, Joanne Atlee and Colette Roland (eds.), pp 53-62, IEEE CS, 2005.

[18] M. Saeki, "Embedding Metrics into Information Systems Development Methods: An Application of Method Engineering Technique", Proceedings of CAiSE'03 Conf., Springer Verlag, 2003, pp.374-389.

[19] H. Mouratidis, P. Giorgini, G. Manson, "Integrating Security and Systems Engineering: Towards the Modelling of Secure Information Systems", *Proceedings of the 15th Conference on Advance Information Systems (CAiSE '03)*, 16-20 June,Velden, Austria.