# Managing Security IT Risk: a Goal-Based Requirements Engineering Approach

Nicolas Mayer
*Public Research Centre Henri Tudor*
*29, av. J. F.Kennedy, L-1855 Luxembourg, Kirchberg*
*Nicolas.Mayer@tudor.lu*

## Abstract

*Security is currently a major concern of Information Systems (IS) and it is generally recommended to take care of security at the early stage of IS development. That's why requirements engineering process seems to be a good step to handle security. In the IT security engineering domain, risk management is one of the most efficient tool, because it permits to compare security needs and costs of security measures. We propose to match some requirements engineering approaches with risk assessment approaches, to deal with IT security of an IS. The aim of this work is to provide some tools and methods to support handling of security during the first stages of a system development. A modeling framework is a cornerstone of such an approach.*

## 1. Introduction

As well as they increase their importance in the business domain, Information Systems (IS) need currently more and more security, due to the number of attacks. Today, security is no more a desirable quality of IT systems, but a required compliance to international regulations. A number of technical answers are available in response to IT security issues. Each of these technical answers has its own level of protection and, also, its own cost. Therefore, one of the challenges is to determine the most suitable compromise between the level of security achieved and its associated cost, to obtain the best ROI (Return On Investment). This compromise should be based on the correct evaluation of the IT risk, which is usually defined by a threat and a vulnerability, with their associated potentiality, and its impact on the business assets of the organization. So it is necessary to adapt the security measures, depending on the risk and its associated components.

The analysis of risks in terms of the links existing between the business assets of an organization and the technical aspects associated with its IS, seems to be best suited for the application of a Requirements Engineering (RE) approach.

## 2. Problem statement

One of the main key to a good alignment between business domain and security of IT structures, is to keep the focus on the assets of the business. *Assets* are anything that has economic value for the organisation and that are central in the realization of business objectives. Figure 1 shows different kinds of business assets in the financial domain. For example, information business assets are customers' name, address and phone number. The process of account management is a core activity of a bank. Business assets are also knowledges such as the ability of doing relevant economic analysis. Otherwise, we are calling IT assets those IT processes and resources of the IS and its environment, linked to the business assets. They are often considered as the "mirror" of the business assets, because many business goals are achieved with assistance of the IS. For example, IT assets are the banking application, managing customers' accounts, and the customers' data, stored in a database and on a server. People encoding data are also considered as IT assets, because they are part of the IS environment and essential in a good account management. IT assets are therefore the IS components (or its environmental ones) needed to be secured, in order to ensure the achievement of the business objectives.

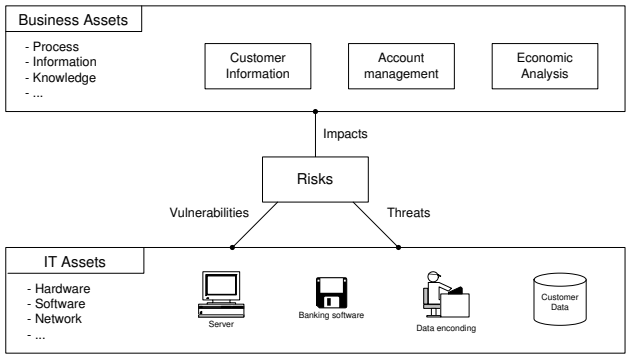


**Figure 1. Risk management concepts**

Assets need to be secured, because they are exposed to

risks. Note that our work only focuses on risks targeting the IS, other risks like financial risks (investment) or organisational ones (hiring of a CEO) are out of the scope. Risk is most often defined by three components :

```
Risk = Threat * Vulnerability * Impact
```

In other words, risk is characterized by the opportunity of exploiting one or multiple vulnerabilities, from one or many entities, by a threatening element using a method of attack, causing an impact on business assets. Figure 1 shows the links between risk components and assets. Vulnerability is a characteristic of the IT system and threat targets the IS, but the impact is reflected on the business of the organization.

A lot of work has already been done in the context of risk management and particularly risk analysis, which is the activity of analysing threat, vulnerability and impact on each component of the system. We can cite some methods based on risk analysis:

- OCTAVE [9], from the USA, developed by the Carnegie Mellon University
- MEHARI [8] from CLUSIF[1] and EBIOS [7] from DCSSI[2], two french methods
- CRAMM [11], developed in the UK

Some risk management methods are most focused on security requirements and control selection, for a standard level of protection :

- BS7799-1:1999 Information Security Management - Part 1: Code of Practice for Information Security [3] ; a british standard, also declined in the ISO 17799 norm
- IT Baseline Protection Manual [10] from BSI in Germany, even specifying security control implementation

These methods are applied in a bottom-up manner, used once the architectural design has been defined. This allows only an "a posteriori" approach of IT security, resulting in a gap between security requirements and business security needs. Our view is that an "a priori" approach of security engineering, based on risk management, could improve IT security.

## 3. Proposed theory

As exposed in Section 2, a lot of work has already been done in the risk management domain, particularly with industrial methods and norms. But there is a mismatch between security methods and IS system development. Our aim is to handle security in the first steps of IS design, during the RE stage.

Risk management methods are considered as semi-formal and are often a good process for a risk assessment. But the product of these methods is informal, most often in natural language, thus creating a gap in automation, evolution, monitoring or traceability of risk management. The aim of the research is then to provide a layer of formalisation in the products of risk management.

### 3.1 Security engineering approach

The proposed approach links first business assets with security engineering. RE is the fitting domain for linking business assets, driven by business goals, with the security engineering domain (Figure 2). On the other side, architectural engineering is the domain linking IT assets, included in the IS architecture, with security engineering. The objective of security engineering is, as already explained, to mitigate risks by providing security requirements.

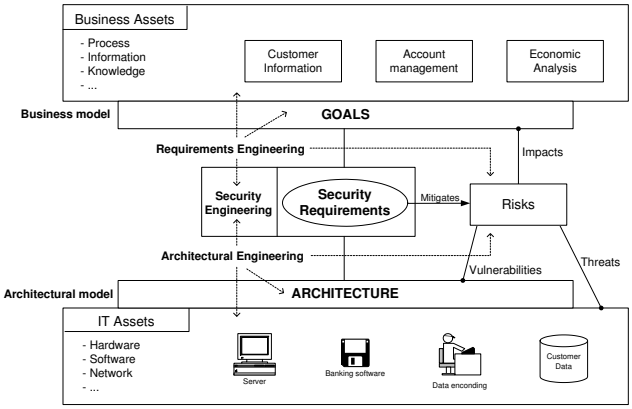


**Figure 2. RE and Architectural Engineering in the IS design process**

The tools used for reasoning about requirements and architectural engineering is respectively architectural and business modeling. Models provide the basis for formalisation, documentation and evolution. Our approach will be however more focused in the RE domain represented in Figure 2, i.e. making the link between business assets overseen by business goals and security engineering used for mitigating risks. RE approach considering security will be presented in the next section, most of them improved by modeling.

### 3.2 Related Work

The RE community has started to be aware of the problem of security in the last years and a lot of security RE

[1] Club de la Sécurité des Systèmes d'Information Français
[2] Direction Centrale de la Sécurité des Systèmes d'Information

approaches have been developed.

- Extensions of UML, especially of the Use Cases models, were proposed to model security aspects, such as Misuse Cases [12] and Abuse Cases [13]. CORAS UML profiles [5] are also considering security risk aspects.
- Problem Frames decomposition of Jackson deals with security, with the Abuse Frames proposal [14].
- The i* framework [17] was developed for the modeling and analysis of organizational environments and their IS. Some security applications of the framework were studied [16] and an extension for handling risk issues was developed [1].
- The KAOS approach [6] has specialized the goal analysis technique to critical system engineering (e.g. safety critical systems), which is adapted for securing critical business assets. Another goal-oriented modeling framework is the NFR framework [15], handling security as a class of non-functional requirements.

The preceding methods and techniques will be investigated and enhanced according to the research objectives. Risk management methods presented before are also naturally a source of interest for the research work.

### 3.3 Expected outcome

Despite many approaches were developed in the domains of risk management and security RE, few approaches integrate the two aspects. The PhD work will first pursue the objective of identifying the IT security and risk management concepts needed to enhance the RE process. It will be then necessary to identify the RE methodologies best suited to integrate the previously identified concepts, for handling IT security as early as possible.

Once all of this preliminary work is done, it is necessary to develop models and methodologies to deal with security and risk management in the early steps of an IS development. A modeling framework seems to be best suited to formalize and exploit these elements. As explained before, being not only a support for analyze and reasoning, it also permits some improvements like (semi-)formalisation or traceability. But it seems unnecessary to completely redesign a new modelling framework, as improving an existing one with risk management concepts should be more relevant. The focus will be more on assets identification and business modeling (i.e. the RE side of Figure 2), but the link with architectural modeling is necessary to complete the process of IS design. A study of existing security standards and references (ISO 15408, ISO 17799, NIST and CERT documents...) to extract technical and organisational requirements can also improve the method, by providing security measures to mitigate the risks, as the outcome of the security engineering process.

The development of a prototype supporting the overall approach is finally considered. Automation and deliverables produced by the process are thus a main part of the expectations and the prototype should be fulfilling them. A case study is then necessary to experience and validate the work.

The improving of such a method, apart from managing security during the first steps of software engineering, is the claim of risk management constituted by the models. Moreover, as already mentioned during the introduction, models can help system designers and managers to improve the ROI of their IS security. Despite the fact that the study will not provide some quantitative method for calculating ROI, having a clear view of assets and safeguards linked to them helps practitioners to deal with security costs.

## 4. Progress

This project research deals with two major scientific domains: RE and risk management. The first step was to do a state of the art of these domains. We studied the most used risk management methods (security experts estimate there is more than 200 risk management methods, so an overall study is inconceivable). The RE domain, being very large and varied, we tried to focus only on our main interests. We investigated mainly the goal-oriented, security driven or business modeling RE approaches. This work of bibliography is still in progress.

As exposed in Section 3.2, some contributions were very close to our approach, but the bibliography denotes that no current work is able to tackle every part of our problem. We are currently interested in collecting some worthwhile RE approaches and try to merge them with risk management methods.

## 5 Acknowledgments

Thanks to my advisors Eric Dubois and André Rifaut for their guidance in this project. The work is partially supported by the Research National Fund of Luxembourg. Part of the research is performed within the context of the LIASIT (Luxembourg International Advanced Studies in Information Technologies) Institute.

## References

[1] P. Gaunard, 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.

[2] J. D. Moffett, B. A. Nuseibeih: *A Framework for Security Requirements Engineering*, Department of Computer Science, YCS368. University of York, UK, 2003.

[3] *BS7799-1:1999 Information Security Management - Part 1: Code of Practice for Information Security*, British Standards Institution, London, 1999.

[4] L. Chung: *Dealing with Security Requirements During the Development of Information System*, 5th International Conference on Advanced Information Systems Engineering, CAiSE'93, Paris, France, June 1993.

[5] R. Fredriksen, M. Kristiansen, B. A. Gran, K. Stølen, T. A. Opperud, T. Dimitrakos: *The CORAS framework for a model-based risk management process*, Proceedings of the 21st International Conference on Computer Safety, Reliability and Security (Safecomp 2002), LNCS 2434, pp. 94-105, Springer, 2002.

[6] A. Dardenne, A. van Lamsweerde, S. Fickas: *Goal-Directed Requirements Acquisition*, Science of Computer Programming Vol. 20, North Holland, pp. 3-50, 1993.

[7] *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)*, Direction Centrale de la Sécurité des Systèmes d'Information (France), February 2004. http://www.ssi.gouv.fr/

[8] *Méthode Harmonisée d'Analyse de Risques (MEHARI)*, CLUSIF, Version 3, Octobre 2004. http://www.clusif.asso.fr/

[9] *Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)*, Carnegie Mellon - Software Engineering Institute, June 1999. http://www.cert.org/octave/

[10] *IT Baseline Protection Manual*, BSI - Germany, October 2003. http://www.bsi.bund.de/english/gshb/

[11] *CRAMM*, CCTA[3] Risk Analysis and Management Method. http://www.cramm.com/

[12] I. Alexander: *Misuse Cases Help to Elicit Non- Functional Requirements*, Position paper for Policy Workshop 1999, Bristol, U.K., November 1999.

[13] J. McDermott, C. Fox: *Using Abuse Case Models for Security Requirements Analysis*, 15th Annual Computer Security Applications Conference, Phoenix, Arizona, December 1999.

[14] L. Lin, B. Nuseibeh, D. Ince, M. Jackson: *Using Abuse Frames to Bound the Scope of Security Problems*, RE'04, Kyoto, Japan, 2004.

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

[16] L. Liu, E. Yu, J. Mylopoulos: *Analyzing Security Requirements As Relationships among Strategic Actors*, 2nd Symposium on Requirements Engineering for Information Security (SREIS), Raleigh, North Carolina, 2002.

[17] E. Yu: *Towards Modelling and Reasoning Support for Early-Phase Requirements Engineering*, Proceedings of the IEEE Int. Symp. Requirements Engineering, Annapolis, Maryland, pp. 226-235, January 1997.

[3] Central Computer and Telecommunications Agency