Design of a Modelling Language for Information System Security Risk Management

Nicolas Mayer, Patrick Heymans, *Member, IEEE* and Raimundas Matulevičius

***Abstract*—Nowadays, security has become one of the most demanded characteristics of information systems. However, the ways to address information systems security still lack consensus and integration. On the one hand, researchers have extended various modelling languages and methods with security-oriented constructs in order to take security concerns into account throughout the development lifecycle. On the other hand, practitioners have developed risk management methods to help estimate the relative importance of security risks and the cost-effectiveness of solutions to tackle them. They are mainly driven by security standards that help practitioners assess and improve the security level of their organisations. Obviously, those two families of approaches should be unified so as to maximise the return on investment of implementing security requirements, and thereby align business and information technology concerns related to security. This is the challenge that our research aims to address. This paper presents a research agenda and describes the first steps that were undertaken to achieve it: an alignment of the terminology in the risk management literature and the elaboration of a conceptual model of the risk management domain. Those results will then be inputs for the next phases, which aim to integrate security and risk management concepts in information system development methods.**

***Index Terms*—Risk Management, Security, Standards, Conceptual modelling, Requirements Engineering**

I. Introduction

During the last twenty years, security concerns have increasingly impacted on the development and exploitation of Information Systems (IS), both in public and private sectors. The pressure is still increasing in many sectors and organisations, where specific regulations impose advanced security Risk Management (RM) practices. This is the case, for instance, with the Sarbanes-Oxley act [29], which concerns the integrity of financial and accounting data, or, in the banking industry, where the new Basel II agreement [30] defines rules which determine the level of "frozen" capital for financial institutions, based on the maturity of their RM activities, including those related to their IS.

In this context, security RM is paramount because it helps companies adopt cost-effective security measures. Indeed, security threats are so numerous that it is impossible to act on all of them because (1) every technological security solution has a cost and (2) companies have limited resources. Hence, companies want to make sure that they adopt only solutions for which Return on Investment (ROI) is positive. This is done by comparing the cost of a solution with the risk of not using it, e.g. the cost of a business disruption due to a successful security attack. In this sense, security RM plays an important role in the alignment of a company's business with its Information Technology (IT) strategy.

IS security RM (ISSRM) methods (e.g. [8], [9], [10], [11]) are practitioner-oriented methodological tools that help organisations make cost-effective decisions related to the security of IS. Feedbacks on the use of such approaches show that they considerably reduce losses caused by security weaknesses of IS. ISSRM methods are generally based around a well structured *process* (see Figure 2). However the *product* of RM is still informal: it typically consists of a natural language document, possibly complemented with tables for structuring the information. This lack of formality prevents the automation (reasoning, evolution, monitoring and traceability) of RM-related information. Another drawback of current ISSRM methods is that they are most often designed for being used *a posteriori*, that is, to assess the way *existing systems* handle risk. Very few approaches [8], [12] try to include RM constructively in IS engineering practices from the very early phases, i.e. Requirements Engineering (RE), on to the subsequent development phases.

On the other hand, researchers have recently proposed various security-oriented (versions of) RE modelling languages and methods [23], [25], [26], [27]. Unfortunately, these languages and methods have seldom been related to RM. Thereby, they have failed to address in a satisfactory way the cost-effectiveness concern which is of utmost importance for practitioners. Indeed, having a modelling language that allows eliciting and representing security attacks is only of partial help. One also needs a method to judge whether the risk is important enough to justify the inclusion of corresponding security requirements in the requirements document (e.g. asking for the inclusion of security control mechanisms in the IS).

As a consequence, integrating RM and security-oriented RE languages appears as a major challenge of contemporary IS research. Addressing this challenge is intended to provide practitioners with the means to align business and IT concerns related to security.

Nicolas Mayer is with the Public Research Centre Henri Tudor, Luxembourg. Moreover, he is currently a PhD student at the Computer Science Department of the University of Namur, Belgium, in the frame of the LIASIT (Luxembourg International Advanced Studies in Information Technologies) institute, Luxembourg. (e-mail: nicolas.mayer@tudor.lu)

P. Heymans and R. Matulevičius are with the PRECISE lab at the Computer Science Department of the University of Namur, Belgium (e-mail: {phe, rma}@info.fundp.ac.be).

Manuscript received February 15, 2007.

In this paper, we present the first steps of the construction of a model-based approach to support ISSRM. This approach will consist of three components: a methodology ([36], [37]), a modelling language and a tool. This paper focuses on the *modelling language*. More specifically, the research question addressed in this paper is: what are the concepts that should be present in a modelling language supporting ISSRM, especially in the early stages of IS development?

In Section II, we will delimit our scope by defining in more detail the notions of risk, risk management, security and IS. Section III suggests a research method to succeed in the definition of an ISSRM modelling language. In Section IV, we survey the literature on security RM and security-oriented RE modelling languages. In Section V and VI, we present our initial results, obtained by performing the first steps of the proposed research method. The last sections summarise our current progress and announces our future works.

II. Basic definitions

The most generally agreed upon definition of *risk* is the one found in [1]. There risk is defined as a "combination of the probability of an event and its consequence" [1]. Following this definition, *risk management* is defined as "coordinated activities to direct and control an organisation with regard to risk" [1]. Depending on the context, RM can address various kinds of issues [34], [35]. For example, risks can be related to the organisation's management (e.g. illness of a key person in regards to the business), finance (e.g. related to investment), environment (e.g. pollution), or security. In this paper, we focus only on *security RM*. Other kinds of risk, such as financial or project risk, are out of our scope.

In the literature, security is understood in (at least) two different manners. Some authors, e.g. Firesmith [15], use the term *security* for what concerns malicious (or deliberate) harm on the IS, and they use the term *safety* for what concerns accidental harm on the IS. These authors use the broader notion of *survivability* to cover both security (in the above sense) and safety. The notion of security that we adopt in this work, and that defines our scope, is broader. It is actually a synonym of survivability according to Firesmith. We decided to use the term *security* because it is the commonly used term in the RM literature [3], [4], [8], [9], [10], [12] for this concept.

The common denominator of all these RM approaches is the notion that there are security objectives to reach (or security properties to respect) for the assets of the organisation. Assets are generally defined as anything that has value to the organisation, and that needs to be protected. Those properties include *confidentiality*, *integrity* and *availability* of information and/or processes in an organisation [4] [1]:

- *Confidentiality* is the property that information is not made available or disclosed to unauthorised individuals, entities, or processes;
- *Integrity* is the property of safeguarding the accuracy and completeness of assets. Accuracy could be threatened by (unauthorised or undesirable) update or tampering. Completeness could be threatened by altering or deletion;
- *Availability* is the property of being accessible and usable upon demand by an authorised entity.

Harm to those properties can have either accidental or deliberate causes. For example, disclosure of confidential information can be made deliberately by an unlawful person, or accidentally by an error in a programme or an employee's mistake. The scope of this work is thus not limited only to *IT* security, which is concerned with hardware, software and network. It also encompasses people and facilities playing a role in an IS and its security (e.g. people encoding data, air conditioning of server room) and that could therefore be the target of risks. The target system of *security RM* will thus be an *IS*, compliant with the following definition: "A system, whether automated or manual, that comprises people, machines, and/or methods organized to collect, process, transmit, and disseminate data that represent user information" [32].

Summing up, the objective of ISSRM is thus to protect essential elements of an IS, from all harm to their security (confidentiality, integrity, availability) which could arise accidentally or deliberately.

III. Research method

When the scope of our work and the basic terminology being established, now we detail the manner in which we intend to answer our research question: what are the concepts that should be present in a modelling language supporting ISSRM?

An approach should be defined to answer this question in a structured way. The language should be based on solid foundations, extracted from sources relevant to ISSRM. Moreover it should take into account advances in existing security modelling language. The research method is presented in Figure 1. It consists of four steps:

Step 1: *Concept alignment.* We start our research by investigating the state of the art in ISSRM. The main goal of this step is to identify the most important concepts of the domain and harmonise the terminology. The main outcomes of this step are (i) a table that highlights the semantic similarities between the terms used in the various approaches, (ii) a glossary of those terms as found in the sources. An excerpt of the table is shown in Table I presented in Section V (the complete table can be found in the technical report [16]). To get a comprehensive view of ISSRM approaches, we consider 4 main kinds of sources: (i) RM standards, (ii) security-related standards, (iii) security RM methods and (iv) Software Engineering (SE) security frameworks.

Step 2: *Construction of ISSRM domain model.* Based on the outcomes of step 1, we define a conceptual model of the ISSRM domain as an UML class diagram. Each concept

[1] Some other criteria might be added [4], like authenticity, non-repudiation or accountability when the context requires but they are usually deemed secondary.

(class, association) is complemented with a definition provided in a separate glossary and obtained by reusing and, if needed, improving the most relevant definitions found in step 1.

Step 3: *Comparison between ISSRM domain model and security-oriented languages*. Various languages are proposed to model security-related aspects of the IS like security-oriented versions of *i** [25] [26], KAOS extended to security [23], abuse frames [22], and misuse cases [20]. However most of those languages appear to overlook RM. In step 3, we assess to which extent this claim holds. We do so by comparing our ISSRM domain model with the existing approaches. Typically, we investigate the meta-models of those languages, looking for those concepts in the ISSRM domain model which are supported and those which are missing. The comparison approach benefit from recent advances in conceptual comparison of semi-formal languages [38]. The main results of step 3 are (i) the selection of one (or more) candidate language(s) for ISSRM modelling (those with the closest match with the ISSRM domain model) and (ii) the identification of improvements to make to the selected language(s), as we foresee that there will be no perfect match.

Step 4: *ISSRM language definition*. Our goal is to propose a (or a set of, if we choose several candidates) language(s) for ISSRM with solid conceptual foundations. Compliance of its constructs with the domain are guaranteed by the previous steps. This last step aims at applying state of the art language definition techniques in order to deliver a high quality language [41]. This involves a formal definition of syntax and semantics [42] in order to support automated reasoning and avoid ambiguity. It also involves taking into account "softer'' properties such as appropriateness of the graphical symbols and structuring mechanisms [39], [40].

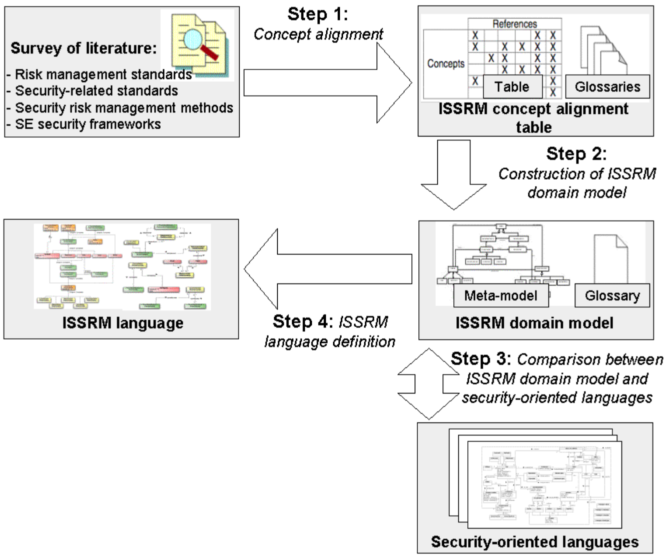
Survey of literature:
- Risk management standards
- Security-related standards
- Security risk management methods
- SE security frameworks
Step 1: Concept alignment
References
Concepts
Table
Glossaries
ISSRM concept alignment table
Step 2: Construction of ISSRM domain model
Meta-model
Glossary
ISSRM domain model
ISSRM language
Step 4: ISSRM language definition
Step 3: Comparison between ISSRM domain model and security-oriented languages
Security-oriented languages

Fig. 1. Global research method

The reader should note that although the process in Figure 1 looks rather streamlined, steps 1-4 are actually conducted in an iterative and incremental way, rather than in a purely sequential way. The results of a first rough iteration already appeared in [36], [37]. However, we have now enriched them by investigating more sources and tightening our research method. Next sections of the paper are mainly focused on the two first steps of the research method.

IV. Survey of the literature

The survey presents first the practitioner state of the art, with an overview of RM objectives and process within RM methods. Then a state of the art of RE security-oriented languages is done for showing main research progress in security during early phases of system engineering. Finally, every source used as input for step 1 of research method is introduced.

A. Risk management process and methods

Application of any ISSRM approach has usually three main outcomes [7]:

- The improvement of IS security;
- The justification of budget and investment for IS security management decisions;
- The indications of trust that customers or partners can have in the IS.

Activities for security management, with respect to risk, focus around a classical process used in traditional RM methods ([2], [7], [8]…). However, the methods do not put the same weights on the same activities. Some methods, for example, are more focused on risk analysis ([8], [9], [10]); others [28], [33] suggest standard security controls (or countermeasures) applied to reach a standard security level. The process can be summarised in 6 main steps (Figure 2).

Process begins with a study of the organisation *context* and identification of organisation *assets*. In this step (a), the organisation and its environment are presented. An overview of the IS is also done. Then, based on the level of protection required for the assets, one needs to determine the *security objectives* (b). Security objectives are often defined in terms of confidentiality, integrity and availability of the assets. The main step of the process is *risk analysis* (c), that elicits what risks are harming assets and threatening security objectives. It consists of identifying risks and evaluating their level in a qualitative or quantitative manner. We speak about *risk assessment* [1] only after the level of analysed risks is compared to the security needs, which are determined during the second step of the process. Once risk analysis is performed, decisions about risk treatment are taken and *security requirements* are determined as security solutions to mitigate the risks (d). Requirements are finally instantiated into security *controls* (e), i.e. system specific countermeasures, that are *implemented* within the organisation (f).

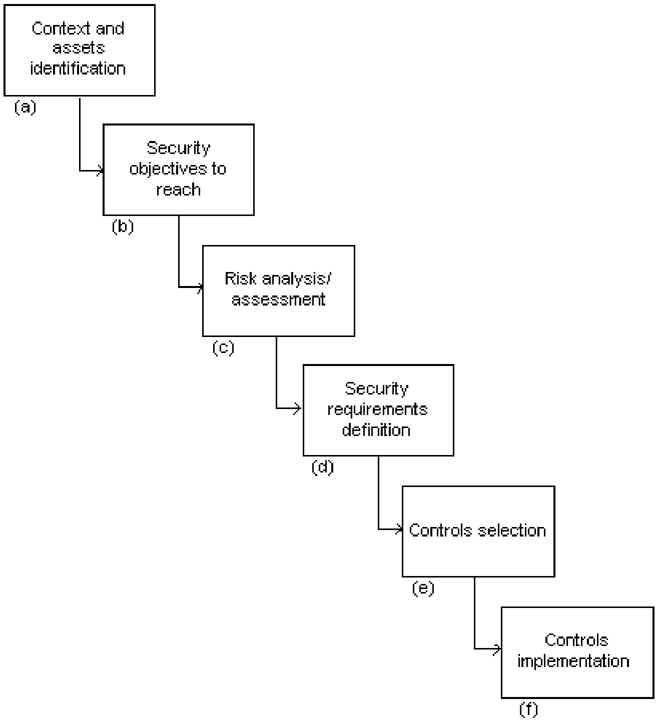
Context and assets identification
(a)
Security objectives to reach
(b)
Risk analysis/ assessment
(c)
Security requirements definition
(d)
Controls selection
(e)
Controls implementation
(f)

Fig. 2. Risk management process

B. *State of the art of RE security-oriented languages*

Many security modelling languages, or most often security extensions to existing languages, were developed to address security in models. Existing approaches based on UML and MDA have been enriched by security modelling facilities (e.g., SecureUML [20]). In misuse cases [21] and abuse case [22], which are extensions of "Use Case" diagrams, the focus is placed on elicitation of new threats and vulnerabilities exploited by malicious actors. The KAOS framework enriches goal-oriented approaches with security aspects by treating attacks as anti-goals [23]. Extensions of the *i** framework are also tackling security problems. For instance, Liu *et al.* [24] represent attacks as softgoals with negative contributions to security softgoals. Formalisation of *i** to deal with security issues is proposed in Secure-Tropos [25], [26]. Furthermore, problem frame extensions [27] are also proposed to handle security issues. However, the approaches generally only deal with security management and do not provide any support for RM activities. CORAS [12] is a rare exception of approaches where RM issues are tackled extending UML. Unfortunately, CORAS is not aligned with ISSRM literature [16] and not connected with early requirements of system engineering.

C. *Presentation and scope of the sources*

The first step of the research method is grounded in a literature survey, including four families that fully support our research scope - *IS security risk management*. The first family is about RM standards. They are high-level references presenting general RM and standing over domain specific RM approaches.

- ISO/IEC Guide 73 [1]: This guide defines the RM vocabulary and guidelines for use in ISO standards. It mainly focuses on terminology, which is of great interest with respect to our research method.
- AS/NZS 4360 [2]: This joint Australian/New-Zealand standard provides a generic guide for RM. The document proposes an overview of RM terminology and process.

The second family of sources consists of (IS/IT) security standards. The selected documents often contain a section that concerns security-specific terminology. Sometimes some RM concepts are also mentioned.

- ISO/IEC 27001 [3]: The objective of this standard is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS), that is the part of the overall management system of an organisation concerned by information security. The terminology related to an ISMS is provided in this reference.
- ISO/IEC 13335-1 [4]: This standard is the first of the ISO/IEC 13335 guidelines series that deal with the planning, management and implementation of IT security. This part is about concepts and models of IT security that may be applicable to different organisations.
- Common Criteria [5]: The Common Criteria (or ISO/IEC 15408) provides a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The first part entitled "Introduction and general model" is important with respect to our research scope.
- NIST 800-27 Rev A [6] / NIST 800-30 [7]: Within the series of publications proposed by the National Institute of Standards and Technology (NIST), the 800-series is about computer security. In this series of publications, NIST 800-27 and NIST 800-30 are the most relevant to the scope proposed in Section II. Terminology and concepts are provided by these standards and are compliant one with the other.

Risk management methods is the third family of sources. In 2004, a CLUSIF[2] study registered more than 200 security RM methods. In this frame we select a representative subset of RM methods based on some recent conferences and studies, like the report "Inventory of risk assessment and risk management methods" [17] from ENISA. Most of the methods are supported by a software tool, but we will focus only on the methodological part of each of them.

- EBIOS [8]: The EBIOS method is developed and maintained by the DCSSI (Central Information Systems Security Division) in France.
- MEHARI [9]: MEHARI is a RM methodology developed by the CLUSIF and built on the top of two other RM methods: MARION [18] and MELISA [19] not maintained anymore.
- OCTAVE [10]: OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is an

[2] http://www.clusif.asso.fr/en/clusif/present/

approach to information security risk evaluations developed by SEI at the Carnegie Mellon University.

- CRAMM [11]: CRAMM is a RM method from UK originally developed by CCTA[3] in 1985 and currently maintained by Insight Consulting.
- CORAS [12]: CORAS (Risk Assessment of Security Critical Systems) was a European project developing a tool-supported framework, exploiting methods for risk analysis and risk assessment of security critical systems.

Finally, the last family concerns SE security frameworks proposed in research publications. These publications are extracted from SE and RE domain, that are of great interest regarding our research scope, and concern safety and security.

- Haley *et al.* [13] and Moffett and Nuseibeh [14] propose a framework for dealing with security requirements engineering.
- Firesmith [15] presents a set of related information models that provides the theoretical foundation underlying safety, security, and survivability engineering.

V. Concepts presentation

A. Set of terms to consider in the concept alignment table

The objective of the first step of the proposed research method is to semantically align the set of concepts related to ISSRM. First task of this step is naturally to precise the range of concept to study. Considering the RM process presented in Figure 2, our modelling language is focused on step (b) to (d). The first activity (step (a)), aiming at identifying business and assets, can indeed be fully supported by existing RE languages [23], [24], [36], [37]. For the two last steps about controls selection and implementation, they are out of the scope of RE activities. Considering steps (b) to (d), the need of models for these steps is checked with the requirements of documentation for “the risk assessment report”, extracted from the ISO 27001 standard [3]. The range of the risk assessment report is indeed defined within the standard as equivalent to the range going from steps (b) to (d) on Figure 2.

Considering the range defined above, the core concept to consider is naturally the one of risk, that will be analysed in depth in this paper. However, risks are highly dependent on and related to (i) security needs of the assets and (ii) risk treatment selected. So their related concepts are also included into the set of concepts to take into account. This fuzzy range of concepts is only a first boundary for performing step 1 of the research method (Figure 1). First step is performed iteratively, instantiating incrementally the fuzzy range of concepts to a defined set of concepts. The final set of concepts elicited will be the one available in the table at the end of step 1 of the research method [16]. Nevertheless, the set of concepts can be reduced or increased afterwards, in case of specific needs from users or new concepts needed for consideration. Then other steps of the research method will be modified incrementally.

B. Overview of the grid

In this section we will illustrate our approach by reporting on the analysis of the central concept – *risk* – as extracted from the sources surveyed in Section IV.C. Other considered concepts could be found in [16]. An emphasis is placed on the definition of *risk* and identification of its components. Other characteristics of risk presented in its various definitions ([7], [8], [15]…), like for example its value or activities acting on it, are not currently considered. Our final outcome being the definition of a modelling language, these characteristics of risk are at this time secondary. At the opposite, risk sub-components or related concepts are directly involved in the definition of the syntax of the language.

1) Risk management standards

As already said in Section II, ISO Guide 73 [1] gives the following definition of risk:

***Risk**: combination of the probability of an event and its consequence*

The AS/NZS 4360 source [2] proposes a very close definition in its glossary:

***Risk**: the chance of something happening that will have an impact on objectives*
NOTE 1: A risk is often specified in terms of an event or circumstance and the consequences that may flow from it.

Both sources are extracted from RM standards and show that a risk is composed of two related elements: a cause, called *event* or *something happening*; and a consequence, also called *impact*. This consideration is valid to all the risk domains. Next we will compare both definitions with the ones from security domain. Our purpose is a further refinement of our analysis.

2) Security related standards

In ISO/IEC 27001 [3], the concept of *risk* is not present in the glossary, but in an excerpt of the standard presenting the risk identification step we find:

*Identify the **risks**.*
1) Identify the assets within the scope of the ISMS, and the owners of these assets.
2) Identify the threats to those assets.
3) Identify the vulnerabilities that might be exploited by the threats.
4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

In ISO/IEC 13335 [4], risk is defined in the glossary in a very close manner in terms of involved concepts:

[3] Central Computer and Telecommunications Agency

***Risk**: the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.*

The analysis of both sources [3], [4], and mainly the definition from [4] which is more explicit than the succession of steps presented in [3], shows it is compliant with [1] and [2] because risk is always composed of a cause and a consequence component. However the definitions introduce some new concepts: *cause* of the risk is presented as the combination of *threat* and *vulnerability* and *consequence* labelled as *impact* or *harm* (Section V.B.5 Table I). The concept of *asset*, which will not be analysed in depth in this section, is also introduced as related to risk. It is defined as anything that has value to the organisation [4].

Common Criteria (CC) [5] defines *risk* with a finer level of granularity:

Threats are categorised as the potential for abuse of protected assets.
*The CC characterises a threat in terms of a threat agent, a presumed attack method, any vulnerabilities that are the foundation for the attack, and identification of the asset under attack. An assessment of **risks** to security would qualify each threat with an assessment of the likelihood of such a threat developing into an actual attack, the likelihood of such an attack proving successful, and the consequences of any damage that may result.*
A threat shall be described in terms of an identified threat agent, the attack, and the asset that is the subject of the attack. Threat agents should be described by addressing aspects such as expertise, available resources, and motivation. Attacks should be described by addressing aspects such as attack methods, any vulnerabilities exploited, and opportunity.

Here the cause of the risk is called *threat* and it encompasses vulnerability unlike ISO/IEC 27001 [3] and ISO/IEC 13335 [4] that define them as related, but separate concepts at the same level. The threat or the cause of the risk in [5] is therefore composed of multiple subcomponents like *threat agent*, *attack method*, *attack*, etc. Details of those subcomponents can be found in [16]. *Threat* in ISO/IEC 27001 or ISO/IEC 13335 has thus not the same sense as *threat* in CC, that is equivalent to the global cause of the risk, encompassing *threat* and *vulnerability*. *Threat* from [3], [4] and *threat* from [5] are thus not aligned in Table 1.

NIST standards also propose a different definition of risk [6], [7]:

***Risk**: The net mission/business impact considering (1) the likelihood that a particular threat source will exploit, or trigger, a particular information system vulnerability and (2) the resulting impact if this should occur.*

In terms of involved concepts, risk is once again defined with the help of 3 components that are *threat source*, *vulnerability* and *impact*. The concept of *threat* is defined as the combination of a threat-source, its motivation (for human threat) and threat-actions, like hacking, social engineering, or system intrusion [7].

The use of the term *risk* in security related standards shows that its definition is more precise than the one proposed in RM standards, but it is nevertheless compliant with ones given in RM standards. *Risk* in security standards is in fact the specialisation, in the frame of security, of *risk* in RM standards. The concept of risk is therefore aligned between the sources in Table 1. However the precision of the components of risk is increased. The consequence of the risk differs only in terms of associated "label" or name, called sometimes *consequence*, *impact* or *harm*, but the underlying semantic remains the same. However the cause of the risk is presented as a composition of elements, which are different between the sources. We can see differences and equivalences in Table 1.

The concept of *asset* is often mentioned in the *risk* definition of security related standards. However it is sometimes associated with the threat [3], sometimes with the vulnerabilities [4] and sometimes with the concept of *attack* [5]. A conclusion is that the concept of *asset* is playing a role in the definition of a risk and should be linked with it. But more investigation about *asset* is necessary to define precisely the relationship among risk, its components and the concept of *asset*. At this stage it will therefore not be included in the alignment table (cf. Table I).

3) Security risk management methods

The definition of risk is also different in each security RM method. EBIOS [8] defines the concept of *risk* as:

***Risk**: Combination of a threat and the losses it can cause, i.e.: of the opportunity, for a threat agent using an attack method, to exploit one or more vulnerabilities of one or more entities and the impact on the essential elements and on the organisation.*

This definition in terms of concepts and relationships between them is aligned with the one of CC (cf. Table 1). The threat represented as the global cause of the risk, is a combination of many subcomponents.

In MEHARI [9], the absence of a glossary is an obstacle to a clear comprehension and alignment of concepts. However, clues can be found for *risk* definition within the method.

*A **risk scenario** is the description of a malfunction and the way in which the malfunction can happen. The malfunction states the potential damage, or the direct deterioration caused by the malfunction, and any indirect consequences. It is usual to speak of a risk situation, where it is understood that the organization is potentially exposed to such a scenario.*
Each scenario will therefore be described as follows:

- *The type of consequence (sometimes in relation with predefined value scale)*
- *The type of resources implicated by the scenario (sometimes in relation with the predefined critical resources)*
- *The types of causes that can lead to the risk situation.*

In MEHARI the term *risk* is used less often than the term *risk scenario* for expressing the concept of *risk*. The cause and the consequence parts of the risk are well respected. The link with resources concerned by the risk scenario is added.

OCTAVE provides the following risk definition [10]:

***Risk**: [...] Risk refers to a situation where a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence.*
It breaks down into three basic components: asset, threat, and vulnerability.

The definition of risk and its components is the same in CRAMM [11]. In this source, the risk is defined using the Figure 3 and followed with the definition:

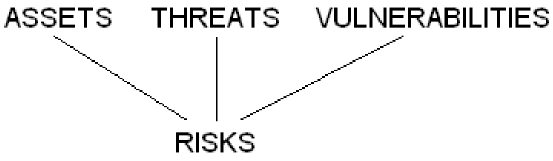

Fig. 3. Risk representation in CRAMM (adapted from [12])

***Risk**: A measure of the exposure to which a system or potential system may be subjected. This is determined by the combination of:*
• the level of threat
• the vulnerability
• the possible loss which may result from such an attack.

Three components compose the risk for sources [10] and [11]: the threat, the vulnerability and the consequence called *loss* or (relative to) *assets*. CRAMM gives clue in its definition of *risk* for defining *attack* in regards to risk. It is the concrete instantiation of the threat using the vulnerability on the target system. Attack is therefore not in the potential domain of RM. Attack is thus not taken into account in the ISSRM concept alignment table. Naturally this definition of *attack* may eventually apply only to CRAMM.

Finally, the CORAS RM method [12] proposes a risk definition, which is highly related to the concept of *unwanted incident*:

***Risk**: A risk is an unwanted incident along with its estimated likelihood and consequence values.*
***Unwanted incident**: An unwanted incident is an event which reduces the value of one or more of the assets*

The use of the term *event* should not be confused with the one in other sources like [1], [2] or [3] designating the cause of the risk. Here *event* actually denotes the impact of the risk on the organisation. Examples of unwanted incidents are "design disclosed to competitor" or "customer loses trust in [the company]" that is characteristic of an impact. A risk in CORAS is defined as an impact with an associated level of potentiality and consequence. Naturally the likelihood of the impact to occur is highly dependant on the cause of the risk. Further analysis of CORAS also introduces elements of the cause of the risk: *threat*, *threat scenario* and *vulnerability* [16]. However, they will not be developed here.

Within security RM methods, the concept of risk is once again not universally agreed. First, RM methods reinforce the conclusion obtained from RM standards that identify a cause and a consequence part in a risk. However a great diversity is provided in the fine-grained definitions of risk and its components. With the new elements obtained from the sources of security RM methods and security-related standards, a tendency is emerging: the cause part of the risk consists of two elements most often called *threat* and *vulnerability*.

4) SE security frameworks

In [14] Moffet and Nuseibeh were inspired by CRAMM and propose the same figure to present risk and its components (cf. Figure 3) associated with the following definitions (their proposal is reinforced by Haley *et al.*[13]):

***Threat**: Harm that can happen to an asset*
***Impact**: A measure of the seriousness of a threat*
***Attack:** A threatening event*
***Vulnerability**: a weakness in the system that makes an attack more likely to succeed*

Firesmith proposes a very precise definition of *risk* [15], which is split into safety risk and security risk. They both are encompassed by survivability risk which is defined as follows:

***Survivability risk** is the potential risk of harm to an asset due to the sum (over all relevant hazards and threats) of the negative impact of the harm to the asset (i.e., its criticality) multiplied by the likelihood of the harm occurring.*

The focus on survivability risk makes clear that the two parts of a risk are characterised by *likelihood* for the cause (with an emphasis on the value of the cause) and *impact* for the consequence. Investigation of definitions and associated information models shows that the likelihood of the risk depends on the likelihood of a threat (for security domain) or hazard (for safety domain) and the existence of (safety or security) vulnerability.

5) Alignment table for risk and its components

Discussion of this section is summarised in Table 1. It shows a proposition of the alignment of the selected concepts related to risk and its components. Five concepts are thus proposed here. They are numbered from (1) to (5), but not labelled for the moment (see Section VI). Other analysed concepts can be found in the technical report [16].

TABLE I
ALIGNMENT OF FIVE CONCEPTS

Reference	(1)	(2)	(3)
ISO/IEC Guide 73 [1]	Risk	Event	Consequence
AS/NZS 4360 [2]	Risk	Event	Consequence Impact
ISO/IEC 27001 [3]	Risk	/	Impact
ISO/IEC 13335 [4]	Risk	/	Harm
Common Criteria [5]	Risk	Threat	Consequence
NIST 800-27 [6] *NIST 800-30* [7]	Risk	/	Impact
EBIOS [8]	Risk	Threat	Impact
MEHARI [9]	Risk Risk scenario	Cause	Consequence
OCTAVE [10]	Risk	/	Impact Consequence
CRAMM [11]	Risk	/	Loss
CORAS [12]	Risk	/	Unwanted incident
Haley et al. [13] *Moffett and Nuseibeh* [14]	Risk	/	Impact
Firesmith [15]	Risk[1]	/	Impact

[1] Firesmith differentiate Safety risk and Security risk that he encompasses by Survivability risk.

Reference	(4)	(5)
ISO Guide 73 [1]	/	/
AS/NZS 4360 [2]	/	/
ISO/IEC 27001 [3]	Threat	Vulnerability
ISO/IEC 13335 [4]	Threat	Vulnerability
Common Criteria [5]	/	Vulnerability
NIST 800-27 [6] *NIST 800-30* [7]	Threat	Vulnerability
EBIOS [8]	/	Vulnerability
MEHARI [9]	/	/
OCTAVE [10]	Threat	Vulnerability
CRAMM [11]	Threat	Vulnerability
CORAS [12]	Threat scenario	Vulnerability
Haley et al. [13] *Moffett and Nuseibeh* [14]	Threat	Vulnerability
Firesmith [15]	Hazard Threat	Vulnerability

In this section we present only one iteration of step 1, which results with alignment Table I. Further activities involve current iteration of the step trying to review, validate, and improve current results. The table is then completed and modified after further analysis of risk components [16].

VI. Construction of ISSRM domain model

Step 2 of the research method (Figure 1) starts with the suggestion of a label for the concept of each column of the table. It takes into account labels proposed in the sources and the analysis performed in Section V. The suggestion is the following:

(1) Risk
(2) Cause of the risk
(3) Impact
(4) Threat
(5) Vulnerability

We propose definitions of risk and its subcomponents as follows:

(1) **Risk**: A security risk is the combination of a threat with one or more vulnerabilities leading to a negative impact harming one or more of the assets. Threat and vulnerabilities are part of the cause of the risk and impact is the consequence of the risk.
Examples: a cracker using social engineering on a member of the organisation, because of weak awareness of the staff, leading to non-authorised access on personal computers and loss of confidentiality and integrity of sensitive information; a thief penetrating the organisation's building because of lack of physical access control, stealing documents containing sensitive information and so provoking loss of confidentiality.

(2) **Cause of the risk**: The cause of a risk is the combination of a threat and one or more vulnerabilities.
Examples: Cracker using social engineering because of lack of awareness; a thief penetrating the organisation's building because of lack of physical access control.

(3) **Impact**: The impact is the potential negative consequence of a risk that may harm assets of a system or an organisation, when a threat (or the cause of a risk) is accomplished. The impact can be described at the level of IS asset (data destruction, failure of a component…) or at the level of business assets, where it negates security criteria, like for example: loss of confidentiality, loss of integrity, unavailability… Impact can provoke chain reaction of impacts (or indirect impact), like for example a loss of confidentiality on sensitive information leads to a loss of customer confidence.
Examples: Password discovery (IS level); loss of confidentiality (business level)

(4) **Threat**: Potential attack or incident which, in combination with one or more vulnerabilities, targets one or more of the IS assets and that may lead to harm to assets. A threat is usually composed of a threat agent and an attack method.
Note: We advocate that sometimes, a risk is more relevant to be described with a global threat, without refining into threat agent and attack method, like for a flood or a component failure.
Examples: Cracker using social engineering, flood, component failure.

(5) **Vulnerability**: Characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of IS security. It could be accidentally or intentionally exploited by a threat.
Examples: weak awareness; lack of access control; lack of fire detection.

The core concept of ISSRM – *risk* – is modelled in Figure 4. A *risk* is *composed of* a *cause* and one or more *impacts*. A given cause can only be related to a given risk (cause is characteristic of risk), but an impact can be related to many risks. *Cause* of the risk *leads to impact*. An impact can be related to many different causes and a given cause can lead to many impacts. Sometimes a relevant impact can be caused by none relevant causes of risk and so contained in none of the risks. The *cause* of a risk *is composed* of a given *threat* and one or more *vulnerabilities*. A given threat can only be related to a given cause of the risk. The *threat exploits* one or several *vulnerability(ies)*. A given vulnerability can be exploited by many different threats and therefore related to many different causes of risk, or being not exploited by any of them.

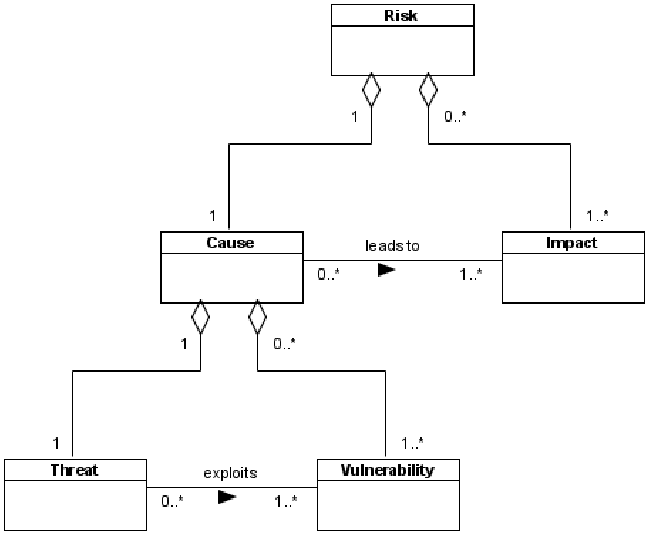

Fig. 4. Core concepts of ISSRM conceptual model

The definitions and the model proposed above can be incrementally refined with the iterative reviews of the alignment table of step 1. For example the introduction of the definitions of attack method or threat agent can improve the definition of threat [16]. Moreover, the task of concepts formalisation brings us some feedback that involves us to refine and improve the meta-model and the definitions. The full meta-model of ISSRM domain is composed of about 15 concepts [16].

VII. Conclusion

In this paper, we suggested a research method to design a modelling language for Information Systems Security Risk Management (ISSRM). This language is targeted at integrating IS development and Risk Management (RM) practices in relation to security. So doing, it is also intended to help align, respectively, IT and business concerns of companies. Those are recognised as important challenges of today's information society.

The research method that we proposed consists of 4 steps:

- Step 1: Alignment of the concepts of ISSRM,
- Step 2: Construction of an ISSRM domain model,
- Step 3: Comparison between the ISSRM domain model and security-oriented languages,
- Step 4: ISSRM language definition.

This paper presents the results obtained through iterations of the two first steps of the research method. It focused on the analysis of the central concept of *risk*. In step 1, after gathering all the definitions of risk found in the selected sources, an analysis of the similarities and differences between them was made. Then step 2 delivered a synthesis in the form of a conceptual model, and proposed new definitions of the concepts, taking into account every contribution from the studied sources.

We agree with Moffett and Nuseibeh [13] that "the meanings of terms in this area are not universally agreed", speaking about risk analysis/management. The diversity of the obtained results [16] shows that this work is useful and relevant before suggesting an (ISS)RM modelling language. It helps identify the concepts used in RM and extract a core subset of them, with clear definitions, before producing the language.

VIII. Future works

Table I, resulting from step 1, should still evolve by considering other security-related methods and frameworks from the state of the art (some sources are already planned to be added [31]). Step 2 will then improve the domain model accordingly. Naturally, our endeavour will also address step 3 and 4 until the definition of the ISSRM language is complete. For this, an accurate confrontation of our domain model with the meta-models of security-oriented languages like Secure Tropos [25], [26], *i** by Liu *et al.* [24], Abuse Frames [27] or KAOS extended for security [23] will take place. Comparison and integration will be based on the methodology defined in [38].

Step 3 is currently work in progress. The method used for identifying the ISSRM concepts supported by a language is close to the one used in step 1. A thorough analysis of reference documents about the language gives clues to understand the underlying concepts. However, languages come with a meta-model which is already a semi-formal representation of the concepts and relationships in the language. We can then suggest an alignment between ISSRM concepts and the studied language concepts. The subset of the language meta-model in line with the ISSRM meta-model can be extracted to have a clear view of the support provided for ISSRM. We are repeating this process for each of the aforementioned languages. The main outcome of this step is naturally a survey indicating which concepts and parts of ISSRM are supported by the existing RE security-languages.

From the conclusions of this survey, step 4 will deliver an ISSRM specific language, most probably by improving the language that will have the best ISSRM coverage. The language definition will be carried out accurately, based on the highest language definition standards [42]. Also, the modelling language will be supported by a tool. This tool will be implemented on top of a meta-CASE environment [43], for extensibility.

Extensibility is indeed a property that we are keen on. It will allow us to keep up with new sources appearing in the literature or standards evolution, and for customising our language in response to specific needs, i.e. creating domain specific languages. A meta-CASE will support extensibility at the tool level. At the method level, extensibility is supported by an iterative and incremental performance of our 4-step process. Of particular interest for extensibility, we point out the correspondence table between the concepts of the studied sources and the concepts defined in our language. We think that this traceability will facilitate the use of our modelling language within any of the studied ISSRM methods by offering a mapping between their respective terminologies.

Still looking at future works, we are also attentive to the emergence of the new ISO 2700X standard family. Those standards will be up-to-date and homogeneously aligned with ISO 900X for the quality domain, and ISO 1400X for the environment domain. The coming ISO 27000 standard about fundamentals and vocabulary for information security management systems will propose new terminological bases for security and RM. Our approach can help standards become more precise, and it has indeed been selected as a reference for the review of ISO 27000 by our national chapter for IS security standardisation[4].

Finally, strategies for validating the work should be defined. Some first internal and external validations have already been carried out by expert practitioners and scientists. However, an obvious threat to validity is the possible subjectivity of the experts' viewpoints, especially regarding terminology. A better level of confidence will be pursued in several complementary ways: (1) with more expert validations, (2) by applying the language in the development and assessment of real IS and (3) by using well accepted ontology [38] to compare and align domain and meta-models.

References

[1] *Risk management – Vocabulary – Guidelines for use in standards*, ISO/IEC Guide 73, 2002.

[2] *Risk Management*, Australian/New Zealand Standard 4360, 2004.

[3] *Information technology - Security techniques - Information security management systems – Requirements*, ISO/IEC 27001, 2005.

[4] *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*, ISO/IEC 13335-1, 2004.

[5] *Common Criteria for Information Technology Security Evaluation version 3.1,* ISO/IEC 15408, August 2005.

[6] *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A*, NIST Special Publication 800-27 Rev. A, June 2004.

[7] *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30, July 2002.

[8] *EBIOS – Expression of Needs and Identification of Security Objectives*, DCSSI – France, February 2004.

[9] *MEHARI (Information risk analysis and management methodology) V3, Concepts and Mechanisms*, CLUSIF, October 2004.

[10] *Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)*, Carnegie Mellon - Software Engineering Institute, June 1999.

[11] *CRAMM (CCTA Risk Analysis and Management Method) User Guide version 5.0*, Insight Consulting – SIEMENS, September 2003.

[12] F. Vraalsen, T. Mahler, M. S. Lund, I. Hogganvik, F. den Braber and K. Stølen, "Assessing Enterprise Risk Level: The CORAS Approach," in *Advances in Enterprise Information Technology Security*, D. Khadraoui and Francine Herrmann, Idea Group Reference, March 2007. ISBN : 978-1599040905

[13] C. B. Haley, J. D. Moffett, R. Laney, and B. Nuseibeh, "A Framework for Security Requirements Engineering," in *Proceedings of the 2006 Software Engineering for Secure Systems Workshop* (SESS'06), co-located with the 28th International Conference on Software Engineering (ICSE'06), Shanghai, China, 20-21 May 2006, pp. 35-42.

[14] J. Moffett and B. A. Nuseibeh, "A framework for Security Requirements Engineering," Department report, Department of Computer Science University of York, UK, 2003.

[15] D. G. Firesmith, "Common Concepts Underlying Safety, Security, and Survivability Engineering," Technical Note CMU/SEI-2003-TN-033, Software Engineering Institute, Pittsburgh, Pennsylvania, December 2003.

[16] N. Mayer, P. Heymans and R. Matulevičius, "Design of a Modelling Language for Information System Security Risk Management," Technical Report, October 2006. Available on http://www.nmayer.eu/publis/DesignISSRM-TR-10-06.pdf

[17] *Inventory of risk assessment and risk management methods*, ENISA, March 2006.

[18] *MARION (Méthodologie d'Analyse des Risques Informatique et d'Optimation par Niveau)*, CLUSIF, 1998.

[19] *MELISA (Methode d'Evaluation de la Vulnerabilite Residuelle des Systemes d'Information)*, Direction des Constructions Navales, 1989.

[20] T. Lodderstedt, D. Basin, and J. Doser, "SecureUML: A UML-Based Modeling Language for Model-Driven Security", *Proceedings of the 5th International Conference on The Unified Modeling Language*, 2002, pp. 426–441.

[21] G. Sindre,A. L. Opdahl, "Eliciting security requirements with misuse cases". *Requirements engineering 10 (1)*, pp. 34-44, 2005.

[22] McDermott, J. and C. Fox, "Using Abuse Case Models for Security Requirements Analysis", *15th Annual Computer Security Applications Conference (ACSAC'99)*, IEEE CS Press, Phoenix, Arizona, 1999.

[23] A. van Lamsweerde, "Elaborating Security Requirements by Construction of Intentional Anti-models". In *Proceedings of the 26th International Conference on Software Engineering (ICSE'04)*, IEEE Computer Society , pp. 148–157, 2004.

[24] 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.

[25] H. Mouratidis, P. Giorgini, G. Manson, and I. Philp, "A Natural Extension of Tropos Methodology for Modelling Security", Proceedings of the Agent Oriented Methodologies Workshop (OOPSLA 2002), Seattle-USA, November 2002.

[26] P. Giorgini, F. Massacci, and N. Zannone, "Security and Trust Requirements Engineering", in *Foundations of Security Analysis and Design III - Tutorial Lectures*, LNCS 3655, Springer-Verlag GmbH, 2005.

[27] 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.

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

[29] *Summary of Sarbanes-Oxley Act*, AICPA, 2002.

[30] Basel Committee on Banking Supervision, "International Convergence of Capital Measurement and Capital Standards. A Revised Framework", *Bank for International Settlements Press & Communications*, CH-4002 Basel, Switzerland, 2004.

[31] A. Avizienis, J.-C. Laprie, B. Randell and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing", *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp.11-33, 2004.

[32] Wikipedia, "Information system". Available: http://en.wikipedia.org/wiki/Information_system

[33] *IT-Grundschutz Manual*, BSI – Germany, 2004.

[34] *Project Management Body of Knowledge*, Technical report, The Project Management Institute, November 2001. http://www.pmi.org

[35] *Environmental management systems - Requirements with guidance for use*, ISO/IEC 14001, 2004.

[36] E. Dubois, N. Mayer, A. Rifaut, and V. Rosener, "Contributions méthodologiques pour l'amélioration de l'analyse des risques", Book Chapter in: T. Ebrahimi, F. Leprévost, B. Warusfel, *"Enjeux de la sécurité multimédia",* Traité IC2 - Information, Commande, Communication, Hermès - Lavoisier, 2006. ISBN : 2746212072

[37] 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

[4] http://www.ansil.eu/

[38] R. Matulevičius, P. Heymans and A. L. Opdahl, "Comparing GRL and KAOS using the UEML Approach", *Accepted at the 3rd International Conference on Interoperability for Enterprise Software and Applications (I-ESA 2007)*, Madeira, Portugal, March, 2007.

[39] D. Moody, "Dealing with "Map Shock"": A Systematic Approach for Managing Complexity in Requirements Modelling", *Proceedings of REFSQ 2006*, Luxembourg, 2006.

[40] D. Moody, "What Makes a Good Diagram? Improving the Cognitive Effectiveness of Diagrams in IS Development", *Proceedings of the 15th int. conf. in Information Systems Development (ISD 2006)*, 2006.

[41] J. Krogstie, G. Sindre and H. Jørgensen, "Process Models Representing Knowledge for Action: A Revised Quality Framework", *European Journal of Information Systems*, 15(1):91-102, February 2006.

[42] D. Harel and B. Rumpe, "Meaningful Modeling: What's the Semantics of "Semantics"?", *IEEE Computer vol.37 n°10*, pp.64-72.

[43] V. Englebert and J. L. Hainaut, "DB-MAIN: A Next Generation Meta-CASE", *Information Systems Journal (special issue on meta-modelling and methodology engineering), 24(2)*, Ed. Lyytinen, K. and Welke, R., pp 99-112, June 1999.