Towards a Measurement Framework for Security Risk Management

Nicolas Mayer[1,2], Eric Dubois[1], Raimundas Matulevičius[2], and Patrick Heymans[2]

[1] CRP-Henri Tudor - CITI
29 Av. John F. Kennedy, L-1855 Luxembourg, Luxembourg
nicolas.mayer@tudor.lu, eric.dubois@tudor.lu
[2] PReCISE, University of Namur,
rue Grandgagnage 21, B-5000 Namur, Belgium
rma@info.fundp.ac.be, phe@info.fundp.ac.be

Abstract. Risk management is currently a key tool for managing Information System (IS) security. In the context of the definition of an IS Security Risk Management (ISSRM) modelling language, we already defined the set of concepts and relationships taking a place in the ISSRM domain within a UML class diagram. To extend this work and to support reasoning at the modelling language level, the objective is now to define the metrics available. A systematic and iterative research method is proposed to determine suited metrics. It consists first of the application of the Goal-Question-Metric (GQM) approach on the domain model. Second a review of the literature aims at completing and validating this first step. The outcome of this work is the enrichment of the class diagram with attributes representing the elicited metrics.

1 Introduction

Security aspects currently play a vital role in Information Systems (IS) and are thus a central issue in their effective usage. In this context, a lot of work has already been done in the IS Security Risk Management (ISSRM) domain and particularly many industrial methods for risk assessment (see e.g., [1–4]) have been recently proposed. They are generally focused on structuring the different steps and activities to perform ISSRM. However, regarding the documents produced as output of these different steps, they are generally informal, most often expressed in a natural language. This lack of formality prevents the automation (reasoning, evolution, monitoring and traceability) of ISSRM-related information.

For a long time, IS engineers are aware about the problems of informal documents. They use 'models' as a way to achieve a better formality and quality in the representation of the knowledge. In our previous work [5], we argued for a modelling component which provides better support to formalise different information and knowledge created and exchanged during ISSRM. The results of ad-hoc extensions of security-modelling languages, presented in [6, 7], has highlighted the need of a structured research method. This research method includes the set-up of an ontology of ISSRM concepts, called domain model, which can act as a meta-model for the targeted modelling language. It has been established during a preceding research work, through a systematic elicitation method presented in [8]. It has then been applied to assess the support of some existing modelling languages with regards to ISSRM in [9, 10].

In this paper we focus on the metrics identification and their integration in the domain model. They are necessary for allowing reasoning at the modelling level. The objective of such a measurement system is to reach the best Return on Security Investment (ROSI) for the studied IS, and so to optimise the alignment between the business of the organisation and its IS security. In this paper, we investigate *what the metrics relevant for performing ISSRM and reasoning about ROSI are*. Our research objective is, first, to propose a systematic manner to define what the metrics to be used in ISSRM are. Second, the application of this research method shall propose a set of metrics to be integrated in our domain model and so in our modelling language.

Section 2 introduces our preceding work about the definition of an ISSRM domain model, together with its set of concepts. Then, Section 3 presents the research method for the definition of the ISSRM metrics. Section 4 and Section 5 are the application of the two steps of the research method, respectively for metrics elicitation and metrics validation. Finally, Section 6 is the enrichment of our domain model with the metrics. The paper ends with conclusion and future work in Section 7.

2 The ISSRM domain model

The objective of ISSRM is to protect assets of an organisation, from all harm to IS security which could arise accidentally or deliberately, by using a risk management approach. Its domain model aims at presenting the different concepts involved and their mutual relationships. In this section we summarise some core definitions of ISSRM concepts, organised in three categories: asset-related concepts, risk-related concepts and risk-treatment related concepts. The domain model, represented as a UML class diagram, can be seen at the end of the paper in Fig. 3. It consists of the set of classes and their relationships, the attributes of the classes being the subject (and the contribution) of the rest of the paper.

Asset-related concepts describe what assets are important to protect, and what criteria guarantee asset security. An *asset* is anything that has value to the organisation and is necessary for achieving its objectives. A *business asset* describes information, processes, capabilities and skills inherent to the business of the organisation, and that has value for it. An *IS asset* is a component of the IS supporting business assets. *Security criterion* characterises a property or constraint on business assets. They are most often confidentiality, integrity and availability, but sometimes, depending on the context, other specific criteria might be added, like non-repudiation or accountability.

Risk-related concepts present how the risk itself is defined. A *risk* is the combination of a threat with one or more vulnerabilities leading to a negative impact harming one or more of the assets. An *impact* describes 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 *event*, in the frame of IS security, is the combination of a threat and one or more vulnerabilities. A *vulnerability* describes a characteristic of an IS asset or group of IS assets, that constitutes a weakness or a flaw in terms of IS security. A *threat* characterises a potential attack or incident, which targets one or more IS assets that may lead to a harm for the assets. A *threat agent* is an agent that can potentially cause harm to IS assets. An *attack method* is a standard means by which a threat agent carries out a threat.

Risk treatment-related concepts describe what decisions, requirements and controls should be defined and implemented in order to mitigate possible risks. A *risk treatment* is the decision of how to treat an identified risk. A *security requirement* is the refinement of a risk treatment decision to mitigate the risk. *Controls* (or countermeasures) are means designed to improve security, specified by a security requirement, and implemented to comply with it.

Regarding our coming modelling language, the current state of the domain model brings out the concepts to be considered. However, it does not provide any information about how to reason with these concepts, and if it is necessary to estimate them. Therefore, the next step is to complete the domain model by introducing the metrics of ISSRM. They shall be added as attributes of the ISSRM class diagram (Fig. 3).

3 Research method for metrics definition

To achieve the objective of defining relevant ISSRM metrics, we propose a research method based on a combination of approaches (Figure 1). The outcome of this research method is the introduction of ISSRM metrics as attributes to the ISSRM domain model.

The first approach, used during Step 1 of the research method, is the Goal-Question-Metric (GQM) paradigm [11]. This approach is used for eliciting metrics in a top-down manner, from general objectives to achieve, to suited metrics to be used for achieving the objectives. Thus, the benefit of using GQM is that we focus on the main objectives of ISSRM to define the metrics. GQM is applied on the ISSRM domain. Therefore, the ISSRM domain model is an input for this step. The application results in GQM models, leading to the set of ISSRM metrics. However, this elicitation work remains subjective and potentially incomplete.

The second approach, used as a validation/improvement of the first step, and appearing in Step 2 of the research method, is based on a survey of ISSRM standards and methods [1–4, 12–15]. This approach is bottom-up, being an analysis of the literature to identify the metrics currently used. For each ISSRM source of the literature studied, a comparison is done between its metrics and those

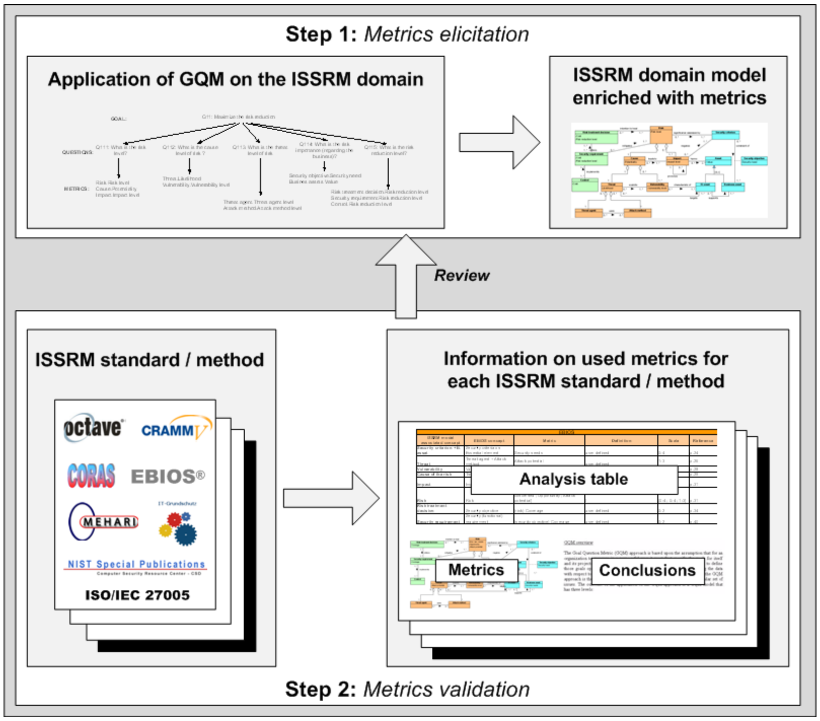
Step 1: Metrics elicitation
Application of GQM on the ISSRM domain
GOAL:
G11: Maximise the risk reduction
QUESTIONS:
Q111: What is the risk level?
Q112: What is the cause level of risk ?
Q113: What is the threat level of risk
Q114: What is the risk importance (regarding the business)?
Q115: What is the risk reduction level?
METRICS:
Risk.Risk level
Cause.Potentiality
Impact.Impact level
Threat.Likelihood
Vulnerability.Vulnerability level
Threat agent.Threat agent level
Attack method.Attack method level
Security objective.Security need
Business asset.Value
Risk treatment decision.Risk reduction level
Security requirement.Risk reduction level
Control.Risk reduction level
ISSRM domain model enriched with metrics
Review
ISSRM standard / method
octave
CRAMM
CORAS
EBIOS®
MEHARI
IT-Grundschutz
NIST Special Publications
Computer Security Resource Center - CSD
ISO/IEC 27005
Information on used metrics for each ISSRM standard / method
Analysis table
Metrics
Conclusions
Step 2: Metrics validation

Fig. 1. Research method for the ISSRM metrics elicitation

defined through GQM. This comparison is summarised in an analysis table. If a metric not identified with GQM is found, it is necessary to evaluate its relevance. Even it can highlight a lack in the GQM study, and thus the GQM models are reviewed and improved considering this new issue, or a justification for the exclusion of the metric shall be provided. This task is iteratively done for every approach identified in the literature [1–4, 12–15].

Once the literature is completely surveyed, leading to the GQM models in their last version, the final set of metrics is introduced in the ISSRM domain model as attributes of the classes.

4 The GQM approach for metrics elicitation

4.1 The GQM approach overview

In the GQM approach, measurement is defined in a top-down fashion [11]. GQM is based upon the assumption that, for an organisation to measure in an efficient way, it must specify the goals for itself and its projects first, then it must trace those goals to the data intended to operationalise them. Finally, it must provide a framework for interpreting the data with respect to the stated goals [11].

The result of the application of the GQM approach is the definition of the measurement system targeting a particular set of issues. The outcome is a GQM model that has three levels: the *goal level*, the *question level* and the *metric level*. Therefore, a GQM model is a hierarchical structure starting with a goal (the goal to be reached). The goal is refined into several questions. Each question is then refined into metrics.

4.2 Application of the GQM framework on the ISSRM domain

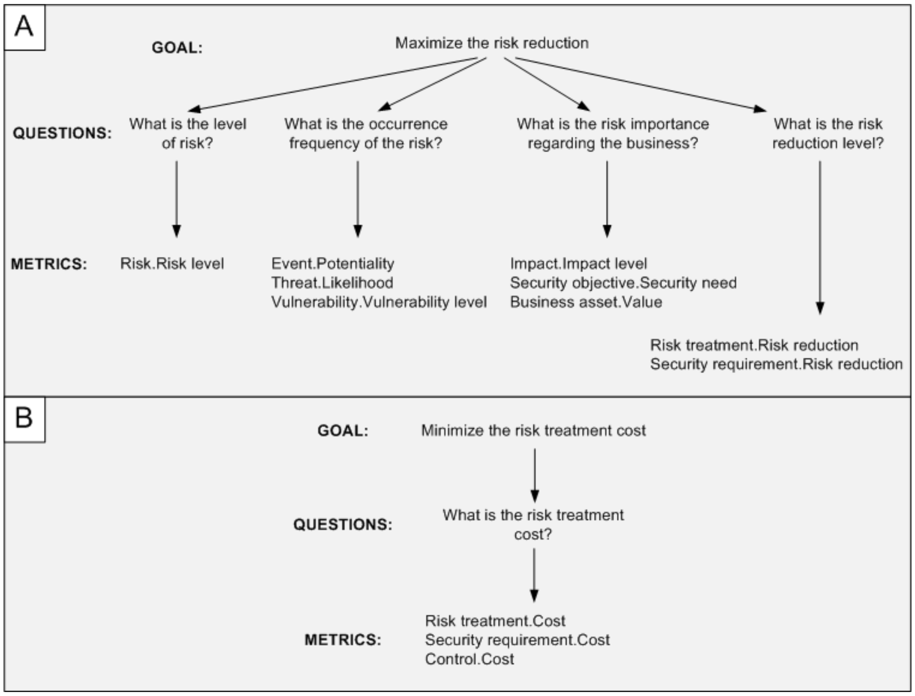
A
GOAL:
Maximize the risk reduction
QUESTIONS:
What is the level of risk?
What is the occurrence frequency of the risk?
What is the risk importance regarding the business?
What is the risk reduction level?
METRICS:
Risk.Risk level
Event.Potentiality
Threat.Likelihood
Vulnerability.Vulnerability level
Impact.Impact level
Security objective.Security need
Business asset.Value
Risk treatment.Risk reduction
Security requirement.Risk reduction
B
GOAL:
Minimize the risk treatment cost
QUESTIONS:
What is the risk treatment cost?
METRICS:
Risk treatment.Cost
Security requirement.Cost
Control.Cost

Fig. 2. GQM models

The main outcome of ISSRM and one of the main motivation is to obtain the best ROSI [16, 13]. Several definitions of ROSI are available [17–19]. Whichever definition is chosen, the following proposition remains valid regarding the ISSRM domain: to maximise the ROSI means to *maximise the risk reduction* when *minimising the risk treatment cost*. Thus, this assumption provides two objectives for the GQM study, which are respectively the two roots of the GQM models (Fig. 2). Considering the concepts of the ISSRM domain model, to maximise the risk reduction involves to know first *what is the level of risk*, depending on its *occurrence frequency* and its *importance regarding the business*. Second, it is necessary to know *what is the risk reduction level*. To minimise the risk treatment cost, it is naturally necessary to know *what is the risk treatment cost*.

From these questions, and based on the set of concepts of the ISSRM domain model (Fig. 3), the related metrics are defined. All of the elicited metrics are represented in the GQM models (Fig. 2) with the following notation: "Class of the ISSRM model.Metric". For example, regarding the treatment cost of risk, we know with regards to the domain model that 3 risk treatment-related concepts are involved. A *cost* metric is thus proposed for each of them to know their respective cost (Fig. 2 part B). It is necessary to note that the GQM models of Figure 2 are the ones obtained after the last iteration of Step 2, as depicted in the research method. They thus represent the final set of metrics. Further explanations about each metric are provided after their validation, in Section 6.

5 Survey of ISSRM approaches for metrics validation

For the ISSRM domain model definition, we surveyed the ISSRM literature [8]. Regarding our metrics validation, we select the subset of the identified ISSRM literature having a methodological part. The approaches focusing on terminology or conceptual aspects of ISSRM are neglected. We thus select 8 sources in ISSRM standards [12–14] and methods [1–4, 15] as the pool of sources to be studied for metrics validation. The complete presentation of Step 2 of the research method about metrics validation can be found in [20]. In this section, we present and comment the metrics analysis table (Table 1) for the ISO/IEC 27005 standard [12], which is the standard for ISSRM. In this table, the concepts are ordered by type, respectively standing in asset-, risk- and risk treatment-related concept category (Section 2). The categories are delimited by a double line in the table.

Table 1. Metrics analysis table for ISO/IEC 27005

	ISO/IEC 27005 [12]		
ISSRM concept	**Concept**	**Metric**	**ISSRM metric**
Asset	Asset	Value	/
Business asset	Primary asset	Value	Value
IS asset	Supporting asset	Value	Value
Risk	Risk	Risk level	Risk level
Event	Event	Likelihood	Potentiality
Impact	Consequence	Business impact value	Impact level
Threat	Threat	Frequency of occurrence	Likelihood
Vulnerability	Vulnerability	Easiness of exploitation	Vulnerability level
Security requirement **Control**	Control	Effectiveness	Risk reduction

The only asset-related concept measured in ISO/IEC 27005 is the concept of asset (in general) (Table 1). The related metric is the *value* of assets. Primary asset and supporting asset, being specialisations of asset in general, are also measured with this metric. Then, the *business impact value* associated to each asset is estimated, based on the *value* of the asset. Risk estimation is based on the successive considerations of threat and vulnerability, leading to event *likelihood*. Combining it with the *business impact value*, it is possible to estimate the *risk level*. Finally, controls from ISO/IEC 27005, which can be aligned with both security requirement and control from our domain model, are estimated according to their *effectiveness*, mainly in reducing vulnerabilities.

In ISO/IEC 27005, as said above, the value of asset in general is estimated for asset-related concepts. In the GQM study (and after the complete review of the ISSRM sources), the focus is rather put on the value of business assets, which is more relevant. IS assets being only the support of business assets, it is worth to consider the value of only business assets. Moreover, in IS security, the value of IS assets (e.g., the replacement cost of a computer) is generally considered as negligible compared to the value of the processed information at the business level (e.g., the client information, the estimates, etc.). Finally, it is necessary to consider the value of business assets for estimating the security objectives and assess the significance of risks, as depicted in the ISSRM domain model (cf. Figure 3). IS assets are not involved in this process. For risk-related concepts, the metrics are very close to those proposed in Section 4. Risk, event, consequence, threat and vulnerability of ISO/IEC 27005 have all an associated metric. Moreover, ISO/IEC 27005 proposes additional characteristics for threat source (equivalent to threat agent in the ISSRM model). For example, it is possible to define the motivation, the capabilities and the resources available of a threat source for a deliberate threat, or some factors that could influence the threat source in the case the threat is accidental. However, such characteristics are not included in the metric analysis table, because they are indicators helping to define frequency of occurrence and the risk level in general, rather than metrics themselves. For the risk-treatment related concepts, the effectiveness of controls is estimated, which has the same objective as risk reduction of security requirements in the ISSRM domain model. The concept of risk treatment is not estimated in terms of effectiveness. Finally, the cost dimension is not needed to be measured in ISO/IEC 27005.

6 Enrichment of the ISSRM domain model with metrics

Elicitation (Section 4) and validation (Section 5) of the metrics result in the improvement of the ISSRM domain model by completing it with the ISSRM metrics.

The first modification of the ISSRM domain model is the introduction of a new concept, necessary regarding the metric of *security need*. This concept is security objective and it represents the application of a security criterion on a business asset, like the confidentiality of patient information or the integrity of a financial process. The security need metric expresses the importance of the security objective concept. It is also interesting to determine the *value* of business assets. Only business assets are estimated in terms of *value*. The *value*

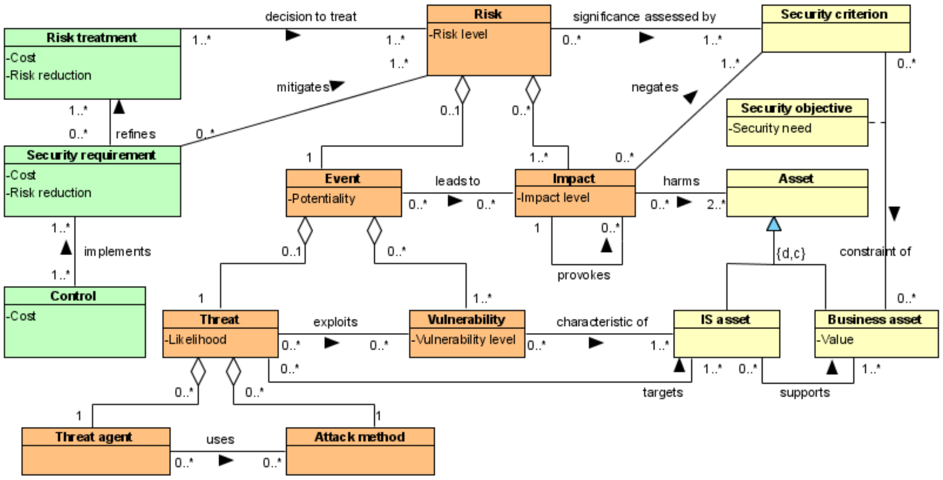

Fig. 3. ISSRM meta-model enriched with metrics

of business assets is used as input to estimate the *security need* of each business asset, e.g., in terms of confidentiality, integrity and availability.

For risk-related concepts, risk is estimated by its level. The *risk level* depends on the event *potentiality* and the *impact level*, these two concepts composing the one of risk. Event is composed of threat and vulnerability. Their respective levels are estimated through *likelihood* and *vulnerability level*. It is necessary to note that threat agent and attack method do not have their own metric representing their level. Only their composition is estimated and this assumption has been confirmed during metrics validation. Some characteristics of threat agents and attack methods can be identified independently, like the motivation and the competence of the threat agent or the kind of attack method (natural, human, etc.), as seen, for example, in ISO/IEC 27005 [12] and EBIOS [1]. However, they can be used as indicators to well estimate the risk-related concepts and mainly the *likelihood* of a threat.

In risk treatment-related concepts, risk treatment and security requirements are estimated first in terms of *risk reduction* performed and second in terms of *cost* incurred. Controls can be only estimated in terms of *cost* (cost of buying a firewall, cost of maintaining it by a security officer, etc.). The *risk reduction* of some controls taken alone has no sense. For example, the *risk reduction* of the security officer maintaining the firewall can not be estimated alone, without considering the global effectiveness of the firewall (described at the security requirement level by, e.g., “Perform network filtering”).

It is necessary to note that this set of metrics is proposed at an abstract level. The metrics can be implemented differently within a method (qualitatively, quantitatively, etc.) [12] or through several metrics, depending on the aim of the method. For example, the *likelihood* metric of threat can be implemented through several attributes of the threat class, the first one being the statistic probability of occurrence of natural threats (in %) and the second one being based on a qualitative level evaluation of human threats. Before implementing these metrics in a method or a tool, it is necessary to think about the best way of using them, depending on the objective and the granularity level wanted. Therefore, this set of metrics has to be considered with an implementation variability.

7 Conclusion and future work

The objective of this paper is to identify and to define a set of metrics for the ISSRM domain with a systematic and scientific approach. First a research method has been defined. Then the application of this research method has been done through the use of the GQM approach on the ISSRM domain and its iterative review with regards to the literature. The result of this paper is the enrichment of the ISSRM domain model with suited metrics.

Although the elicited metrics are validated through literature analysis, their testing in a real case would provide a concrete instantiation and validation of their relevance. An assessment of the metrics is now finished in the frame of an ISO/IEC 27001 certification [21], where ISSRM is at the core of the standard. The metrics proposed were suited in this context and the organisation obtained the certification. The validation should also be a continuous process, through the assessment of other measurement frameworks like [22].

As part of the next step of our future work, the metrics will be integrated into the developed modelling language. Experimentation of the modelling language will help to check the usability of the metrics. The development of a supporting software tool for the language is also important.

References

1. DCSSI: EBIOS - Expression of Needs and Identification of Security Objectives. http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html, France (2004)
2. CLUSIF: MEHARI 2007 (MEthode Harmonisée d'Analyse du Risque Informatique). https://www.clusif.asso.fr/fr/production/mehari/, France (2007)
3. Alberts, C.J., Dorofee, A.J.: OCTAVE Method Implementation Guide Version 2.0. Carnegie Mellon University - Software Engineering Institute (2001)
4. Insight Consulting: CRAMM (CCTA Risk Analysis and Management Method) User Guide version 5.0. SIEMENS (2003)
5. Mayer, N.: Managing security IT risk: a goal-based requirements engineering approach. In: RE'05 Doctoral Consortium, in conjunction with the 13th IEEE International Requirements Engineering Conference (RE'05). (2005)
6. Mayer, N., Rifaut, A., Dubois, E.: Towards a risk-based security requirements engineering framework. In: Proceedings of the 11th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'05). (2005) 83–97

7. Dubois, E., Mayer, N., Rifaut, A., Rosener, V.: Contributions méthodologiques pour l'amélioration de l'analyse des risques. In Ebrahimi, T., Leprévost, F., Warusfel, B., eds.: Enjeux de la sécurité multimédia (Traité IC2, série Informatique et systèmes d'information). Hermes (2006) 79–131
8. Mayer, N., Heymans, P., Matulevičius, R.: Design of a modelling language for information system security risk management. In: Proceedings of the 1st International Conference on Research Challenges in Information Science (RCIS '07), Ouarzazate, Morocco (2007) 121–132
9. Matulevičius, R., Mayer, N., Heymans, P.: Alignment of Misuse Cases with security risk management. In: Proceedings of the 3rd International Conference on Availability, Security and Reliability (ARES '08), Symposium on Requirements Engineering for Information Security (SREIS '08). IEEE Computer Society (2008) 1397–1404
10. Matulevičius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P., Genon, N.: Adapting Secure Tropos for security risk management during early phases of the information systems development. In: Proceedings of the 20th International Conference on Advanced Information Systems Engineering (CAiSE '08). Springer (2008)
11. Basili, V.R., Caldiera, G., Rombach, H.D.: The goal question metric approach. In: Encyclopedia of Software Engineering. John Wiley & Sons, Inc. (1994) 532–538
12. ISO/IEC 27005: Information technology – Security techniques – Information security risk management. (2008)
13. Stoneburner, G., Goguen, A., Feringa, A.: NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology, Gaithersburg (2002)
14. Bundesamt für Sicherheit in der Informationstechnik: BSI Standard 100-3 Risk analysis based on IT-Grundschutz (September 2005)
15. Vraalsen, F., Mahler, T., Lund, M.S., Hogganvik, I., den Braber, F., Stølen, K.: Assessing enterprise risk level: The CORAS approach. In Khadraoui, D., Herrmann, F., eds.: Advances in Enterprise Information Technology Security. Idea group (2007) 311–333
16. ISACA: CISA Review Manual 2006. Information Systems Audit and Control Association (2006)
17. CLUSIF, Groupe de travail ROSI: Retour sur investissement en sécurité des systèmes d'information : quelques clés pour argumenter (2004)
18. Sonnenreich, W., Albanese, J., Stout, B.: Return on security investment (ROSI): A practical quantitative model. In Fernández-Medina, E., Castro, J.C.H., Castro, L.J.G., eds.: WOSIS, INSTICC Press (2005) 239–252
19. Microsoft: The Security Risk Management Guide. (2004)
20. Mayer, N.: Information system security risk management metrics definition, http://www.nmayer.eu/publis/ISSRMmetrics-TR-11-06.pdf. Technical report, CRP Henri Tudor (2008)
21. ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements. (2005)
22. Houmb, S.H., Georg, G., France, R., Bieman, J., Jürjens, J.: Cost-benefit trade-off analysis using BBN for aspect-oriented risk-driven development. In: Proceedings of the 10th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS'05), Shangai, IEEE Computer Society (2005) 195–204