A Language for Multi-Perspective Modelling of IT Security: Objectives and Analysis of Requirements

Anat Goldstein and Ulrich Frank

Institute of Computer Science and Business Information Systems,
University of Duisburg -Essen, Universitaetsstr. 9, 45141 Essen, Germany
{Anat.Goldstein,Ulrich.Frank}@uni-due.de

Abstract. Effectively protecting information systems is a pivotal responsibility of (IT) management, which faces many challenges: technological complexities, business complexities, various stakeholders and conflicting requirements. Yet, there is no holistic modelling approach that comprehensively addresses all these challenges, while accounting for technical, organizational and business aspects. This paper analyzes the requirements of such a comprehensive modelling method for IT security design and management. We argue that enterprise modelling is most suitable to serve as a foundation for such an approach. We apply a method for developing domain specific modelling languages (DSML) that is chiefly based on a structured analysis of use scenarios including prototypical diagrams. It is supplemented by requirements found in literature. Our analysis results in 23 requirements that should be satisfied by the targeted modelling method. These results are intended to serve as a foundation for discussion and discursive evaluation by peers and domain experts.

Keywords: IT security, information security, enterprise modeling, MEMO, DSML.

1 Introduction

The relevance of information technology (IT) security is undisputed in research and practice. It is assumed that the importance of this topic as well as the attention that it experiences in the public will continue to increase mainly as a result of the many threats caused by Internet connectivity and the extensive use of communication and distribution of software services, but also with the increased pressure to follow respective laws and regulations.

Effectively protecting information systems is a pivotal responsibility of (IT) management, which faces many challenges:

- *Increasing technical complexity* as a result of more distributed computing, cloud computing and frequent technological changes. This stresses the need for solutions that are general and not unique for specific technology [1, 2].
- *Increasing risks* by the further upgrading of criminal attackers, who become more sophisticates with time [3, 4]. Apart from criminal attackers, unsatisfied employees as well as careless or insufficiently trained employees may also cause damages intentionally or unintentionally.

M. La Rosa and P. Soffer (Eds.): BPM 2012 Workshops, LNBIP 132, pp. 636–648, 2012.

- *Increasing organizational complexity*: as more business processes as well as financial transactions become automated, a growing number of stakeholders (employees, customers, etc.) receive access to digitized resources and new dangers arise from incorrect use or misuse of systems [5, 1].
- *Increasing pressure to justify the costs* associated with IT security: IT management is required to perform both technical evaluation of alternative solutions and evaluation of their impact on the business competitiveness [6, 7].
- *Communication and cooperation barriers*: language barriers between technical (e.g. IT professionals) and business (e.g. corporate governance) perspectives makes communicating IT security measures more difficult [5, 2, 8].
- *Dealing with conflicting requirements*: high levels of security vs. low levels of costs, high levels of flexibility vs. robust solutions and so forth.

These challenges stress the need for methods and tools for supporting IT management with designing, realizing and managing appropriate IT security systems. According to our conception, an IT security system comprises all technical, organizational and managerial aspects that are required to provide an appropriate level of protection of those resources represented in an information system. Hence, a respective method for protecting information systems does not only need to cover technical aspects of IT security. In addition to that it should also account for behavioral, economic, business and managerial aspects.

An analysis of the state of the art shows that there is a considerable amount of research on various aspects of IT security. However, each one of these streams is isolated from the others and focuses on single aspects only. So far there seems to be no approach which aims at supporting a *holistic view* that integrates the various streams. Also, the majority of respective research is focused on technical aspects. There are only few approaches that consider human factors, e.g. [23] or economic aspects.

Against this background, our research is aimed at a holistic method that integrates the aforementioned technical, organizational, business and behavioral aspects. For this purpose it should provide effective support for mastering the following tasks:

1. Assessing and reducing risks that originate both from within the organization (unsatisfied, careless or untrained employees) and from its outside.
2. Overcoming the increasing technical and organizational complexities, resulting from pervasive distributed computing, frequent technological changes, automation of business processes and growing access to digitized resources.
3. Fostering the participation of non-technical stakeholders (e.g. managers, users)
4. Relating IT security to business, for example, by allowing the analysis of the impact of IT security on business and by allowing cost-benefit analysis.
5. Designing and implementing IS security infrastructures, for example, using automatic creation of security related policies and code fragments.

Each of these tasks is related to one or more perspectives of the enterprise, namely, organization, information systems or strategy perspectives. Accounting for these different perspectives requires a common conceptual framework that covers technical,

business and social aspects. Enterprise modelling provides an obvious choice for this purpose: An enterprise model integrates conceptual models of information systems, (e.g. object models) with conceptual models of the surrounding action system (e.g., business process models). However, so far, languages for enterprise modelling [11,14,15] lack specific concepts for modelling security aspects. Thus, we intend to enhance an existing method for enterprise modeling with concepts to represent relevant issues for IT security. Analyzing the requirements for such a method is of crucial importance – and at the same time a remarkable challenge. It might seem as a straightforward approach to ask prospective users for their needs, e.g. for the properties they would want to see with a corresponding DSML. However, due to the novelty of such an artifact, most prospective users will be overburdened with imagining what they can expect from it. This paper is aimed at presenting an elaborate analysis of requirements to be satisfied by DSML for supporting IT security management. It is supplemented by requirements found in literature.

The remainder of this paper is arranged as follows. In the following section we outline how multi-perspective enterprise modelling can be augmented with concepts to represent IS security aspects. In section 3 we discuss related literature. Next, in section 4, we analyze the requirements of the targeted IT security modelling method – based on the literature and based on use-scenarios we derive specific requirements for this method. We present our conclusions in section 5.

2 Outline of the Targeted Approach

Analyzing, developing, using and managing business information systems is a challenging task that requires the active participation of stakeholders with different professional backgrounds. Hence, there is need to effectively reduce complexity, to provide a foundation for implementing software and to coordinate the contributions of different stakeholders. Enterprise modelling has evolved as an approach to address these challenges by enhancing conceptual models of information systems (e.g. an object model) with those of the respective action systems (e.g. business process models or strategy models).

2.1 Multi-Perspective Enterprise Modelling (MEMO)

MEMO includes a high-level conceptual framework that represents a “ball park view” on an enterprise 25]. It is composed of three *generic perspectives* (i.e. strategy, organization, information system) each of which can be further detailed into various *aspects* (e.g. resource, structure, process, goal). The framework serves as a starting point for identifying perspectives that require further attention. To allow for more elaborate analyses, each selected perspective is associated with a set of diagram types. Each diagram type is associated with a domain specific modeling language (DSML). Different from general purpose modelling languages like the ERM or the UML, a DSML includes domain-specific concepts and features a domain-specific graphical notation. Thus, it promises to increase modelling productivity, to improve model

integrity and to foster the comprehensibility of models. Currently, MEMO includes DSMLs for resource modelling [9], for modelling IT infrastructures [10] organization modelling [11, 12] and for modelling strategic aspects [13]. So far, security-related aspects have not been addressed explicitly. Nevertheless, various DSML within MEMO include concepts that are relevant for IT security management.

The reason for choosing MEMO over other enterprise modelling methods such as ARIS [14] or ArchiMate [15] is based on the following considerations: First, it is based on a flexible language architecture [16]. The language architecture consists of a meta meta modelling language [11] and an extensible set of DSMLs, the semantics and abstract syntax of which is specified using the meta meta modelling language. All DSML that are part of MEMO are integrated through common concepts. The language architecture allows for extending existing languages or for adding new DSML (for example MEMO has been extended to support Risks, Controls and Indicators). Second, MEMO provides support for method engineering and is supported by corresponding (meta-) modelling tool, MEMO Center [16, 17]. Last, but not least, in contrast to commercial approaches like ARIS, the specifications of MEMO and its meta models are freely available and documented in several publications.

2.2 Enhancing Enterprise Modelling with Security Aspects

A multi-perspective enterprise model covers many aspects that are subject of IT security management, such as IT resources (e.g. application systems, components, networks etc.) or organizational roles and organizational units. In addition to that, models of the organizational strategy and of business processes allow for analyzing costs and benefits related to particular IT security measures. Therefore, our approach is aimed at enriching the existing DSMLs with additional, security-related concepts and – if required – to add a further DSML that focuses solely on specific IT security aspects. Fig. 1 illustrates the extension of enterprise models with IT security aspects.
As a consequence, it should enable to model security-related issues on various levels of abstraction, serving different perspectives. For example: A department manager may be especially interested in avoiding negative impact on the performance of business processes he is in charge of. By enriching the representation of a business process with security-related information on an appropriate level of abstraction (e.g. by avoiding too much technical detail), the department manager gets a better idea of what to expect from investments into security management. In addition to that, conceptual models of IT security systems serve as a blueprint for implementing (i.e. at best: generating) corresponding software and for organizational re-design.

3 Related Work

Related work can be grouped into two main categories: work that emphasizes the need for a holistic approach and approaches to model technical aspects of IT security.

3.1 Holistic Security Approaches

There are only few papers that identify the need for a holistic approach for handling IT security in organization. [3] for example, recognizes several dimensions that should not only be considered but also integrated in order to create a secure environment. Among these dimensions are: Strategic/corporate governance, organizational, policy, best practice, ethical, legal, personal/human, technical and auditing. He does not, however, provide any method for identification nor integration of these dimensions. [5] suggests a security management framework for e-commerce that takes into account three dimensions: Society, Technology and Business, throughout all phases of the system lifecycle. However, this framework offers a high-level method, that defines a set of activities for the development of security but it does not provide tools or computer-based support for the implementation and integration of these activities and for their alignment with other aspects of the organization. [6] also recognize a need for a comprehensive approach for information systems security analysis and design (IS-SAD) and suggest incorporating risk analysis and organizational analysis based on business process modelling (BPM). After surveying an extensive list of available BPM techniques they conclude that none of these techniques alone could support IT security analysis and design.

3.2 IT Security Modelling

There is an extensive work that focuses on dedicated modelling approaches to IT security [18,19,1,20,21,22]. SecureUML [8] and SECTET [18] are UML extensions that focus on role-based access control (RBAC). [19] use UML to represent organizational aspects (that is, RBAC) as well. [1] and [2] provide extensions to UML that focus on business process management. [20] develop an extension of BPMN that supports modelling authorization of business processes and allows automatic derivation of authorization policies. [21] introduces UMLSec, an extension of UML that enables developers to formally describe security issues and to identify security errors during the development of information system. [22] present a model based security risk analysis, using CORAS diagrams, which are based on UML. While these approaches are usually aimed at facilitating communication between different stakeholder and providing tools for automatic creation of security-related software, are focused each on a specific aspect of IT security or intended only for supporting software developers.

4 IT Security Modelling: Requirement Analysis

Developing an IT security modelling method requires the specification of corresponding language concepts, either as an extension of existing DSML or as a new DSML. Developing language concepts implies the need for analyzing corresponding requirements. However, analyzing requirements for DSML is a challenging task.

The rest of this section is focused on analyzing the requirements that the IT security modelling language (ML) should satisfy. These requirements will eventually guide the development the DSML.

4.1 General Requirements for IT Security Modelling

A holistic method that will improve the development of comprehensive IT security solutions should account for technological aspects, human/organizational aspects, business aspects and financial aspects. As discussed above, these aspects are (separately) covered by the existing literature and prevalently include topics such as security risk analysis, security policies, security requirements analysis and IT measurements (firewalls, protocols, encryption methods, access control methods). A holistic IT security method should therefore include concepts that are represented by these various security aspects. This is summarized into the first requirement that should be fulfilled by an IT security method,

Requirement 1 - The method should include concepts to describe IT security aspects from various perspectives: technical, human, organizational, business and financial. It should therefore include concepts of other enterprise MLs to support references to respective models that describe aspects of the organization, business processes and IT.

There are many papers that stress the importance of improving the communication and interaction between different stakeholders during the design and management of IT security in organizations (e.g. [22], [2] and [23]). Most of these papers recognize the need for different levels of abstraction when it comes to specifying security requirements, allowing the description of high levels security requirements without getting into technical details. This is important especially because usually managers, who possess a high level perspective of the business processes and functionality, have little knowledge about security issues [2]. Different levels of abstractions can be used not only for differentiating between general and detailed levels of security requirement specifications but can also differentiate between different perspectives of the enterprise: strategic (goals) , organizational (role based access control, security of business processes), technological (vulnerable IT resources, IT measurement) and between different IT security tasks that are under the responsibility of different stakeholders such as security risk management, meeting IT security standards and regulations and cost analysis. This leads us to define the second requirement.

Requirement 2 – facilitating communication and support of different stakeholders: the aimed method should allow for representation of different levels of abstraction and of multiple perspectives specific for the different stakeholders of the IT security design and management. Each perspective should correspond with specific concepts and abstractions from the stakeholder's relevant domain.

Methods for the design of IT security should support the integration of security concerns throughout all the phases of the system lifecycle from requirements analysis to design, implementation, testing and deployment [23, 5, 2, 1, 4]. As indicated by [4], [21] and by [8], most security requirements are added as an afterthought, only

after functional requirements analysis has been completed. Thus, we define a third requirement that a method for IT security should fulfill.

Requirement 3 – the aimed method should support all phases of the enterprise's system development lifecycles. IT security issues should be considered already in the initial stages of system requirement analysis. Identified security requirements can be later enriched with technical details in the design phase and eventually used for derivation of security related code fragments.

4.2 Specific Requirements for IT Security Modelling

The three requirements above are high-level or general requirements. While they are Information-security-specific, they are not necessarily intended for MLs.

In order to collect further specific requirements that should be satisfied by IT security MLs, it might seem reasonable to ask prospective users about their needs and expectation from the targeted DSML. However, due to the novelty of such an artifact, it will be difficult for most prospective users to imagine what they can expect from it. To address this challenge, we follow a use scenario development approach, presented in [24], which has evolved from the development of various DSML, e.g. [12]. According to this approach we use modelling scenarios from the past and also create further possible modelling scenarios to identify IT security specific needs. We supplement each scenario with a prototypical diagram type that may build on an existing ML or that has been created for the purpose of analyzing requirements. For each diagram type we develop a list of exemplary questions that the diagram should answer. These questions help us illustrate the purposes a diagram should serve and recognize specific requirements that should be satisfied by our ML. With respect to preparing for a corresponding modelling tool, it is helpful to classify these questions into three types: if these questions can be answered through an automated analysis (in case a corresponding tool is available), they are marked with an **A**; if answering them can be partially supported by an automated analysis, they are marked with a **P**; and if they are subject to human interpretation/analysis only, they are marked with a **H**. These questions are relevant with respect to the targeted level of detail/formalization, the language specification should satisfy and the intended functions of a respective modelling tool.

Due to space limitation we will present only one scenario that focuses on an IT Resource diagram. A full list of scenarios can be found in [26]. The IT Resource diagram allows the representation of the enterprise's IT resources: the software, hardware and network elements composing the organization's information systems. This is a primary diagram of MEMO Information Technology Modelling Language (ITML). Since most security requirements as well as security controls are related to IT resources, this diagram has an important role in describing IT security aspects and in designing IT security infrastructure.

We present an illustration of an augmented IT Resource diagram (Fig. 1) accompanied by illustrative questions it should help answering.

- Which security requirements are related to an IT resource? **A, H**
- Which counter-measure is related to the security requirement? **A, H**
- What is the cost of adding a security measure resource? **A, H**
- How is a security measure implemented? **A, H**
- What is the number of attack attempts on an IT resource? **A**
- What is the number of successful attempts? **A**
- What is the average number of attack attempts per year on a resource? **A**
- Who is allowed to use/access a resource? **A, H**
- What is the justification for purchasing a certain security measure? **A, H**
- Which business processes are affected by attack on the IT resource? **A, H**

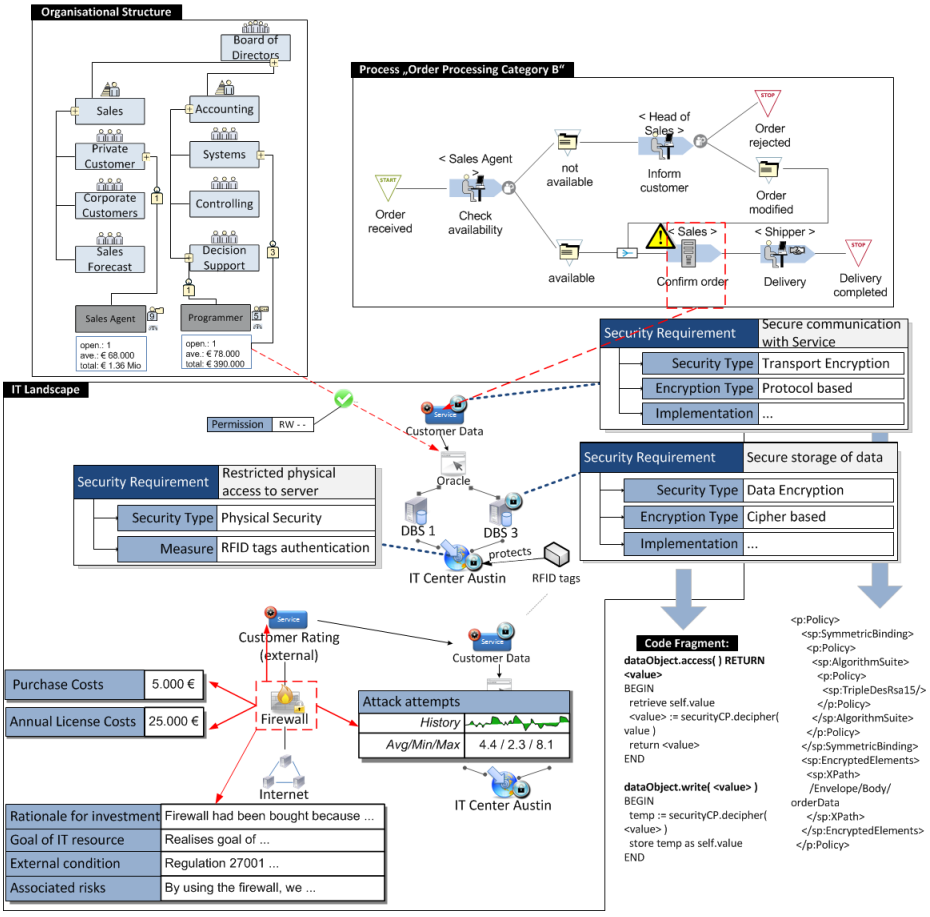

Fig. 1. Illustration of augmented IT resources chart

We derive corresponding requirements that should be satisfied by our ML:

Requirement 4: It should be possible to define security requirements for IT resources (e.g. customer data is confidential and thus should be protected) and to describe the

security measures used in detail (e.g. using cipher based encryption). This implies that a *protection* association is required. This association can be used to indicate that one IT resource is intended to protect another IT resource.

Requirement 5: There should be support for cost-benefit analyses of security measures. For example it should be possible to analyze the effectiveness of a chosen security measure based on the history of attack attempts, to compare the prevented losses against the implementation costs and to justify the acquisition.

Requirement 6: The ML should support different levels of abstraction of security requirements, ranging from high-level, general, definition of security controls to low-level definition of technical details of encryption methods, cipher settings, communication protocols and specific access control policies. Based on the detailed and formal specifications, it should be possible to generate code fragments, web-service descriptors, access control policies, or access tables for databases and applications. This is a specialization of *Requirement 2*.

Requirement 7: It should be possible to define for each IT resource who is responsible for it, who is allowed to access it and their permissions (read, write, execute, delete).

4.3 Requirements Derived from Other Scenarios

The following requirements were derived from further scenarios, which due to space limitations are not presented here. The scenarios include extensions to existing MEMO diagrams: Business Process diagram, Organizational structure, business process map and object model. An additional scenario is related to security risk analysis and requires the definition of a new type of diagram – security risk analysis diagram.

Security Risk Analysis Related Requirements
Requirement 8: The ML should support activities like risk analysis, risk mitigation and evaluation. Thus, it should include the key concepts of the security risk management domain, namely: *asset*, *threat*, *threat-source*, *vulnerability*, *counter-measure* and *impact*. The ML should enable to assign vulnerabilities to assets, to define threat-sources and the vulnerabilities they can exploit (threats they create), to assign probabilities to threats and the impact they have, to match counter-measures to vulnerabilities, and to analyze their cost and benefit.

Requirement 9: The assets mentioned above are IT resources such as data, software or hardware, which are the core concepts of the IT perspective, represented by the MEMO ITML. Thus, the IT security ML should be integrated with the ITML. This will enable connecting security concepts with IT resources for example, connecting a vulnerability to an IT resource or connecting a counter-measure to the IT resource which is used to resolve a vulnerability.

Requirement 10: There should be concepts that support comparing different counter-measures against threats and for performing cost-benefit analysis. It should be possible to indicate the selected measures.

Requirement 11: It should be possible to collect information about attack history, i.e. statistics on the occurrence of threats (instance level).

Business Process Related Requirements

Requirement 12: Integration between the business process perspective and the IT perspective is required so that it would be possible to: 1. associate an activity with its vulnerable assets (IT resources); and 2. associate an activity with selected (IT) counter-measures. These associations should allow for cost and impact analysis of the damage/implementation.

Requirement 13: It should be possible to link activities with threats and vulnerabilities. Thus, the ML should be integrated with concepts from the business process diagram (i.e. activities), provided by MEMO OrgML.

Requirement 14: It should be possible to link activities with users who: 1. are authorized to perform them (based on their position, role, belonging to business unit…); 2. might interfere with their execution.

Requirement 15: It should be possible to indicate that two activities should be performed by different users, that is, two different instances of the same role.

Process Map Related Requirements

*Requirement 16***:** It should be possible to assign detailed security requirements to a business process.

*Requirement 17***:** It should be possible to evaluate the total cost of protecting the various activities of a process type.

*Requirement 18***:** It should be possible to analyze the financial impact of the realization of security risks within a process.

Requirement 19: It should be possible to indicate that an association between two process types has security implications. For example, to indicate that two associated business processes, which share information, comply with different security regulations (since they occur in different countries).

Requirement 20: The ML should provide concepts that enable a detailed description of the security needs in order to allow filtering and representation of different types of security requirements. For example to filter only the process types that are affected by a specific regulation.

Requirement 21: It should be possible to add an indication of security requirements on the instance level as well, for example, in a case where the same process is conducted in several countries with different regulations

Organization Structure Related Requirements

*Requirement 22***:** The ML should allow defining access rights for the different positions, roles and business units with respect to data resources. The formal definition of permission sets allows the automatic derivation of access control

policies, such as RBAC, which is supported by many software platforms. Thus, the modelling tool should support automatic access control policy generation.

Object Model Related Requirements

Requirement 23: The ML should allow defining that objects of a certain class should be encrypted or that a specific attribute should be encrypted.

5 Conclusions

This paper is creates a foundation for a method for supporting IT management with designing, realizing and managing appropriate IT security. The domain of IT security is interwoven with technical, organizational and managerial aspects. These aspects are required to provide an appropriate level of protection of IT resources. Thus, we argue that a multi-perspective enterprise modelling method such as MEMO provides a suitable foundation for an IT security method. Using an approach that is based on augmented use scenarios, we identified 23 requirements that should be satisfied by the modelling method. This list of requirements builds a foundation for designing language concepts that are suited for multi-perspective modelling of IT security aspects. To the best of our knowledge this is the first comprehensive requirement analysis for such a method. The requirements were reviewed by a number of researchers in the field as well as practitioners, who confirmed their necessity and comprehensiveness. We intend to continue validating these requirements with more prospective users in the near future.

One question that arises from the identified requirements is whether we should define a new, IT security designated DSML or we should enrich the existing DSML supported by MEMO (ITML and OrgML) with concepts to support IT Security. On the one hand, IT security concepts do not have a right to exist on their own – they are always associated with IT resource, business process or with organizational positions/roles. This is also stressed by the above presented diagrams, showing that IT security concepts are closely related to existing diagram types. On the other hand, IT security concepts that are used to describe risk analysis (e.g. vulnerabilities, threats, threat-source, likelihood, impact) are not a natural part of the usual tasks involved in the process of IT resource modelling or in business process modelling. While IT resource diagram might be easily enriched with the concept of 'vulnerability', it is harder to decide which diagram should be enriched with concepts of threat, threat-impact or likelihood. Thus, we intend to follow a twofold approach: extending existing DSMLs as well as defining a new DSML to handle security risk analysis concepts.

An IT security modelling method does not have to address all the requirements which were identified in this document. However, the list of requirements describes the scope of the modelling method. At the same time, this list of requirements is not meant to be complete. The requirements are based on the analysis of use scenarios that seem particularly interesting. There are certainly more use scenarios some of which will result in further requirements.

Our next steps are: 1. validate the requirements with further prospective users, mainly with IT managers; 2. develop language specifications that satisfy the requirements; 3. address a number of use scenarios with respective process models to form specific modelling methods; and 4. develop a corresponding modelling tool based on MEMO Center.

References

1. Rodriguez, A., Fernandez-Medina, E., Piattini, M.: Security Requirements with a UML 2.0 Profile. In: The First International Conference on Availability, Reliability and Security (ARES 2006) (2006)
2. Nakamura, Y., Tatsubori, M., Imamura, T., Ono, K.: Model-driven security based on web services security architecture. In: 2005 IEEE International Conference on Services Computing (SCC 2005), vol. 1, pp. 7–15 (2005)
3. Von Solms, B.: Information Security – A multi-dimensional Discipline. Computers and Security 20, 504–508 (2001)
4. Premkumar, T., Stubblebine, S.: Software engineering for security: a roadmap. In: ICSE 2000, The Future of Software Engineering. ACM, New York (2000)
5. Zuccato, A.: Holistic security management framework applied in electronic commerce. Computer and Security 26, 256–265 (2007)
6. Kokolakis, S.A., Demopoulos, A.J., Kiountouzis, E.A.: The use of business process modelling in information systems security analysis and design. Information Management & Computer Security 8(3), 107–116 (2000)
7. Birch, D.G.W., McEvoy, N.A.: Risk Analysis for Information Systems. Journal of Information Technology 7, 44–53 (1992)
8. Lodderstedt, T., Basin, D.A., Doser, J.: SecureUML: A UML-Based Modeling Language for Model-Driven Security. In: 5th International Conference on the Unified Modeling Language, pp. 426–441 (2002)
9. Jung, J.: Supply Chains in the Context of Resource Modelling. ICB Research Report, Universität Duisburg-Essen, No. 5 (2006)
10. Kirchner, L.: Cost Oriented Modelling of IT-Landscapes: Generic Language Concepts of a Domain Specific Language. In: Desel, J., Frank, U. (eds.) The Workshop on Enterprise Modelling and Information Systems Architectures, pp. 166–179 (2005)
11. Frank, U.: The MEMO Meta Modelling Language (MML) and Language architecture. ICB Research Report No. 43, Universität Duisburg-Essen, Essen (2011)
12. Frank, U.: MEMO Organisation Modelling Language (OrgML): Requirements and Core Diagram Types. ICB Research Report No. 46, Universität Duisburg-Essen, Essen (2011)
13. Frank, U., Lange, C.: A Framework to Support the Analysis of Strategic Options for Electronic Commerce. Arbeitsberichte des Instituts für Wirtschafts- und Verwaltungsinformatik, Universität Koblenz-Landau, No. 41 (2004)
14. Scheer, A.-W.: ARIS—Business Process Modeling, 3rd edn. Springer, Berlin (2000)
15. Lankhorst, M.: Enterprise Architecture at Work: Modelling, Communication and Analysis. Springer, Berlin (2005)
16. Frank, U.: Multi-Perspective Enterprise Modeling: Foundational Concepts, Prospects and Future Research Challenges. Accepted for publication in Software and Systems Modeling
17. Gulden, J., Frank, U.: MEMOCenterNG. A full-featured modeling environment for organisation modeling and model-driven software development. In: 22nd International Conference on Advanced Information Systems Engineering, Hammamet (2010)

18. Alam, M., Hafner, M., Breu, R.: A Constraint based Role Based Access Control in the SECTET A Model-Driven Approach. In: 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services, article 13. ACM, New York (2006)
19. Shin, M.E., Ahn, G.-J.: UML-Based Representation of Role-Based Access Control. In: 9th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 195–200 (2000)
20. Wolter, C., Schaad, A.: Modeling of Task-Based Authorization Constraints in BPMN. In: Alonso, G., Dadam, P., Rosemann, M. (eds.) BPM 2007. LNCS, vol. 4714, pp. 64–79. Springer, Heidelberg (2007)
21. Jürjens, J.: UMLsec: Extending UML for Secure Systems Development. In: Jézéquel, J.-M., Hussmann, H., Cook, S. (eds.) UML 2002. LNCS, vol. 2460, pp. 412–425. Springer, Heidelberg (2002)
22. Braber, F., Hogganvik, I., Lund, M.S., Stolen, K., Vraalsen, F.: Model-based security analysis in seven steps—a guided tour to the CORAS method. BT Technol. J. 25(1), 101–117 (2007)
23. Giorgini, P., Massacci, F., Mylopoulos, J., Zannone, N.: Modeling security requirements through ownership, permission and delegation. In: Proceedings of the 13th ICRE 2005 (2005)
24. Frank, U.: Outline of a Method for Designing Domain-Specific Modelling Languages. ICB Research Report No. 42, Universität Duisburg-Essen, Essen (2010)
25. Frank, U.: Multi-perspective enterprise modeling (MEMO): Conceptual framework and modeling languages. In: 35th Annual Hawaii International Conference on System Sciences (HICSS), Honululu, HI, pp. 72–82 (2002)
26. Open Models - IT Security Scenarios, `http://openmodels.wiwinf.uni-due.de/node/204/`