IT Security Risk Analysis based on Business Process Models enhanced with Security Requirements

Stefan Taubenberger[1,2], Jan Jürjens[1]

[1] Open University, Computing Department, UK
[2] MunichRe, Munich, Germany.

Abstract: Traditional risk analysis approaches are based on events, probabilities and impacts. They are complex, time-consuming, and costly, and have limitations regarding the data and assessment quality: First, security events have to be identified often without much methodological guidance, making the process prone to errors and omissions. Second, concrete probability values for these events usually have to be provided, and these are not available in practice to a satisfactory degree of precision and reliability. We propose an approach for risk analysis based on business process models enhanced with security requirements and information about critical processes as well as organizational and system boundaries. This approach bypasses these limitations: security risk events can be derived from the business process models together with the security requirements, and probabilities do not have to be provided. The approach is illustrated using a business process model derived from business practice.

Keywords: Risk assessment, risk analysis, IT security assessment, business process models.

1 Introduction

Increasingly, companies and also governmental organizations suffer from information technology risks caused by malicious or negligent events as well as inappropriate process designs related to authorization, access control or segregation of duties. Examples for such events are the loss of two data discs of 25 million child benefit records in the United Kingdom [6] or the data theft of 45.7 million credit card numbers by hackers at TJX a retailer located in Massachusetts USA [3]. Examples for inappropriate process designs are the Société Générale trading loss incident [11] or the collapse of the Bearings Bank in 1995.

With traditional risk analysis approaches, information technology risks often cannot be adequately identified and evaluated because of limitations inherent to these approaches which are based on security events and associated probabilities: Security events are difficult to identify in a way that guarantees correctness and completeness of this process. Probabilities in practice are difficult to estimate with sufficient degree of precision and reliability. In addition, multiple events (happening in parallel or in sequence) could lead to a range of possible impacts within a range of probabilities, while these impacts may themselves occur only with certain probabilities. This results in a rapid decrease of precision and reliability of the overall risk probability.

Risk analysis approaches using business process models and security requirements (such as [4]) provide an approach for evaluating information technology risks which may overcome these limitations. Mostly existing approaches proceed as follows [7]:

- Identification of business processes and their actors

- Identification and valuation of assets
- Identification of security requirements resp. vulnerabilities and threats
- Assessment of risks
- Proposal, design and implementation of countermeasures

However, the phases "identification of security resp. vulnerabilities and threats" as well as "assessment of risks" of existing approaches have limitations. Mostly the approaches identify and use events and probabilities like in traditional approaches with their limitations. Furthermore security requirements are checked against a repository of safeguards like procedures or case studies [7] or a matrix [20] mapping security safeguards to security requirements. But the existing approaches do not check operational systems regarding the adherence to security requirements (as we will discuss in more detail in Section 1.1 below). In order to improve on this state of the art, the following research questions arise:

- What is the best level of detail to check or monitor the adherence of security requirements of different systems (self-developed and standard applications) in business processes at a given point of time to evaluate IT security risks?
- Are security requirements and risks directly linked and does a security risk always infringe security requirements? E.g. does a physical security risk infringe a security requirement of a business process?
- Do we have a common understanding of security requirements? What are the main attributes of security requirements for evaluation purposes and should technical implementation details be described?
- Are security requirements positive or negative descriptions like in the software engineering domain where e.g. misuse cases or abuse cases describe unwanted behaviour and how close are they aligned with the software engineering domain?
- Can security requirements already consider unknown future risks and how to determine the companies' ability to detect and prevent these risks?

This paper describes first steps towards developing a risk analysis approach which will eventually aim to address these questions. The objective of our approach is to assess current IT security risks of a company in a time-efficient manner without having to identify specific events and probabilities by validating the adherence to security objectives and requirements of data as well as assessing security process maturity. Our approach takes into account:

- the level of criticality of processes – events occurring in the particularly critical processes would cause substantial impact to the company,
- the adherence to security objectives and requirements of data used in these processes at a given point in time – non-adherence would lead to events causing damage. If the security objectives (high level security specifications) and requirements (detailed specifications) are met then implicit impacts of events are mitigated because measures are in place,
- and the ability of IT security processes to deal with security events – the detection and prevention of events.

What's new about our approach is that operational systems are checked against security requirements on basis of predefined security concepts. Our expectation is that the risk analysis results derived using our proposed approach will be at least as good as the traditional approaches using events and probabilities, because security objectives and requirements provide a prioritization of attack targets and detailed security specifications for review. An empirical validation of this assumption is planned for future work (e.g. by extending existing results such as [25]). In addition, using our

approach, critical assets as well as weaknesses in the process and system implementation can be identified at the hand of the business process models.
Our approach has been developed on the basis of significant industrial experience in auditing and evaluating IT processes and systems by the lead author, and reflects some of the problems of testing and evaluating IT security. Based on the practical experience, we recognize the following two use cases: First, to evaluate current IT security risks of a subsidiary or parts of a company for audit planning purposes and second, to evaluate IT security risks of a non-affiliated company to decide about insurance coverage (when the company which performs the risk assessment is a reinsurer, as in the case at hand). In both cases one needs to particularly focus on high risks or high-risk areas, in order to either audit them, or to exclude them from the insurance. But to evaluate the IT security risks in current industrial practice, only limited and incomplete information is available such as network diagrams, systems descriptions, business continuity plans or audit reports. In addition, the assessment has to be conducted in a short period of time (approx. 2-3 days) and to rely on textual information that might not be completely correct or trustworthy.

1.1 Related work

Business process models enhanced with security requirements: Instead of determining single events as in traditional approaches with their limitations [21,12,13], it can be beneficial to first specify the security requirements of the company at hand [4]: The information technology risks of a company are not only determined by single events but also by the level of security required from a business perspective, regulatory or statutory requirements and applicable laws as well as risk to infrastructure [4]. In the related work using business process models and security requirements for information security risk analysis one can find three areas with slightly different objectives.

First, there are approaches that use security requirements to design or verify workflow systems or business processes. Some of these approaches are focused on creating secure business processes or workflows based on security requirements [8,1]. Other approaches propose to analyze security requirements on business processes [20] or verify the consistency of workflow implementations against security policies [18]. All these approaches focus on creation or analysis of security requirements with business processes or workflows to define secure processes.

Second, there are approaches focusing on the analysis and design of information systems (IS) security on the basis of business models or organizational models. The main idea of these approaches is to analyze the organization and the security of systems and then to conduct a risk analysis to design security measures. Some of the approaches in this area support the analysis of the organization to define security requirements [10,15], but not the security analysis. Other approaches [2,9] concentrate on computer security but do not integrate business processes or risk analysis. The approaches in this area lack of a combination of risk analysis and business processes or do not fully support the IS security analysis and design [14].

The approaches in the third area, which are most relevant, define and assign security requirements to business process models and aim to determine risks and appropriate countermeasures. Halliday et. al. [5] proposes to conduct a business driven risk analysis with high-level business processes using risk scenarios and security objectives. Rodriguez et. al. [19] extends the BPMN (Business Process Modeling Notation) to specify security requirements within business process models. Thoben [23] proposes a risk analysis approach comparing the effect of a threat on the workflow system element

to a specified security requirement. Hermann and Hermann [7] use $MoSS_{BP}$ – a framework to specify security requirements and analyze business processes regarding their fulfillment – and Object-Oriented Security Analysis in order to facilitate the automated realization and design of security requirements of business processes. Furthermore there are approaches that use also business process model like e.g. Rainer et al. [17], Suh and Han [22] or Neubauer [16]. We could not build on these approaches when developing the approach proposed here for a variety of reasons, for example that they are based on a traditional risk definition which suffers from the limitation discussed in the introduction, re-engineer existing processes which is time consuming, costly and not always feasible for a risk analysis of operated systems, are heavyweight and time-consuming to apply and learn [25], or stop at the stage of proposing countermeasures without the possibility to extend the risk assessment process further. The main difference between our approach and existing ones is that we identify data processing activities in the business process and check the operated systems against basic security concepts regarding the adherence of security requirements.

Security modeling: There has been a lot of other work towards security modeling, including security design models [26-29] and security requirements elicitation [30,31]; however, this work does not yet seem to have been applied to IT auditing of IT security risks in a business (and in particular insurance) context.

2 IT risk analysis with data security requirements and business process models – description of the approach

In the following, we present our proposed approach that was evaluated by using real-world business process models of two different companies in a study conducted. The approach consists of different stages – identification, definition and assessment – (see figure 1) using available business process models. The approach consists of two parts. In the first part, the current security state is evaluated against security objectives and requirements of data of critical business processes. This indicates that events occurring will not cause a material impact in regard to the specified security objectives and requirements as basic countermeasures are implemented. In the second part, the underlying security processes are assessed regarding their maturity. The maturity level should indicate whether the organization has processes to handle, detect and prevent security incidents in the case of occurrence. Our approach is not described in every detail because of space limitations. In particular, the second part of our approach – maturity of security processes – is not included in this paper.

As stated in [24, p.3], "A business process is widely defined as a structured flow of activities, which supports business goals and is facilitated by data and resources." In our approach we concentrate on activities and data, development-time and run-time elements of a business process [24]. Activities describe the tasks to be executed in a business process to achieve the objectives of the process and data presents a business object that can be created, accessed or changed within process activities. In the used business process modeling tool ADONIS, a business process model is a detailed description of a business process consisting of activities, decisions, sub-processes, used resources etc. The business process modeling notation used in the ADONIS tool consists of the following notation elements (see Figure 1 for an example):

- A triangle and cycle represent the start and end of a process.

- Rectangles represent the activities of the process. Each rectangle is labeled with the name of the activity and can contain the activity number and responsible for the activity as well as above the used system. Activities are tasks to be executed at that moment. Their granularity can vary regarding the requirements of the model.
- Diamonds represent decision points. A decision point has one predecessor and two relations where one must be true. A decision point can also be numbered.
- Arrows between modeling objects e.g. rectangles define the flow of activities and decisions in the process.
- A blue triangle with an arrow represents a subprocess. Subprocesses can be used if the same activities are carried out several times in a process or to structure a process.
- A hexagon represents a trigger that is an event that causes the start of the process.

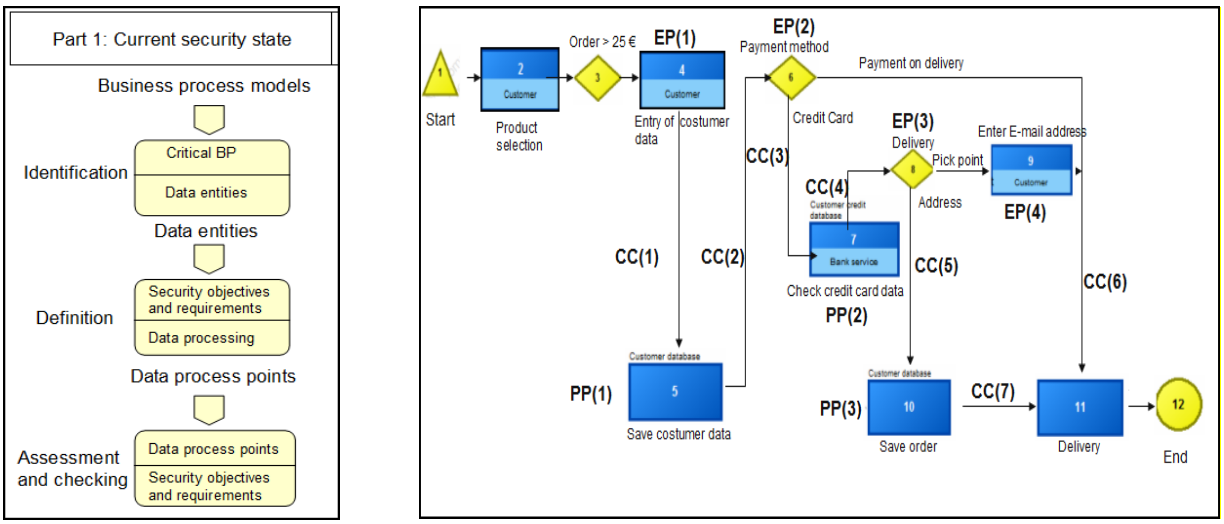

Figure 1. IT risk analysis approach, business process model (order process) with EP, PP and CC

In ADONIS it is also possible to model risks, controls and the organization of a company but this additional elements are not considered in our approach as this information is mostly not incorporated in the models, risks are not static and probabilities not known. The business process flow of figure one is a real world order process for clothing via the internet. Orders below 25 Euros are not possible and the customer can pay via credit card or on delivery. After the complete entry of the customer data and the payment method the order is processed and the goods will be delivered to the customer. The approach is described based on this process flow.

Identification stage

In the identification stage the evaluation of the criticality of the business process and the identification of the data units of critical processes have to be conducted.

The criticality of the business process is determined by the required availability level and is dependent on the business of the company and the objective of single processes. The required availability level – assessed on the basis of the impact of a complete breakdown of the process – is evaluated in relation to all business processes at the company with a qualitative scale e.g. high, middle, low and with the aid of the business

impact analysis if available. The order process via internet is assessed as critical (rating high) as the company creates their turnover via this process.
Data entered and saved in systems as well as exchanged via different channels is a set of information. This information is vital for a process to accomplish the objective of a process activity respectively the complete process. Therefore we use this data processing for evaluation purpose. This data used in the process can be grouped or is already grouped by process activities. We identified the following data entities in the order process: *customer data* and *payment data.* Criteria's and indicators for data entities are decision points and activities in the process as different data or information is used.

Definition stage
In this stage the security objectives and security requirements of the data entities are determined, to identify critical data entities of the business process as well as having a reference – the security requirements – for comparing the current state of security. In addition the entry and process points as well as the communication channels of data entities of the business process are identified. An explanation of these points follows in the next paragraph.

The security objectives for data are determined according the information security objectives – confidentiality, availability and integrity. We use the ISO/IEC FDIS 13335-1 definition for the security objectives and have derived thereof a rating to classify between security levels. Our rating of the data security objectives is based on a qualitative scale. For integrity we distinguish between "accurate", "accurate and complete" and "accurate, complete and accountable", for confidentiality between "no access restriction", "internal access restrictions" and "single user restrictions" and for availability between "immediately available", "within the next 24 hours" and "within the next day".
To determine whether already implemented countermeasures sufficiently support the data security objectives, security requirements have to be specified. In our proposed approach security requirements are detailed specifications regarding the implementation of countermeasures to adhere to security objectives. Currently we do not specify the security requirements in detail because further work is required on this issue. Especially a validated definition of security requirements for the assessment purpose is needed. For determining the security objective level of the data entities some implicit requirements and dependencies have to be considered like the necessity of complete and accurate customer data for the delivery of goods or explicit rules that customer data has to be protected because of privacy laws. The security objective rating for the identified data entities is as follows:

Customer data:	int. = average;	conf. = internal;	avail. = immediately
Payment data:	int. = average;	conf. = confidential;	avail. = immediately

The next task in this stage is to identify entry and process points as well as the communication channels of data entities in the business process model. Entry and process points as well as communication channels specify data system entries, storage and processing of data as well as the transmission of data. With these data process points we are going to evaluate the current level of integrity and confidentiality of data. We defined these data process points as:
Process points (PP): The process point specifies the activity where data is permanently saved electronically or modified (processed). This can be also an entry point.

Communication channels (CC): Communication channels specify the transmission of data between process activities. The data transmission can be across organizational borders, geographic locations or between departments.
In the order business process model we identified the EP, PP and CC depicted in the business process model in figure one.

Assessment and checking stage
In this stage the EP, PP and CC are evaluated regarding basic security concepts - access control, authorization, data validation and communication (authentication and encryption) - to evaluate the adherence to the security objectives integrity and confidentiality. The implementation of the basic security concepts access control, authorization, data validation and communication are rated with different levels e.g. for authorization none, read, execute/process, write/update and full control. Table 2 contains the rating for each data process point (EP, PP and CC) of the basic security concepts.

Table 2. Rating of EP, PP and CC of the order process

Entry points (EP)	Access control & accountability	Authorization (access right)	Data validation
EP(1): customer data	unauthenticated	none	Value verification and completeness
EP(2): Payment data (Payment method)	unauthenticated	none	Value verification
EP(3): customer data (delivery)	unauthenticated	none	Value verification and completeness
EP(4): customer data (e-mail)	unauthenticated	none	Value verification and completeness
Process points (PP)	Access control & accountability	Authorization (access right)	Data validation
PP(1): customer data (costumer database)	System user	Write	none
PP(2): Payment data (credit card database)	System user	Execute	Value verification and completeness
PP(3): customer data (costumer database)	System user	Write	none
Communication channels	Authentication	Encryption	
CC(1): customer data	External unauthenticated partner	None	
CC(2): customer data	External unauthenticated partner	None	
CC(3): payment data	External unauthenticated partner	Standard encryption	
CC(4): payment data	External unauthenticated partner	None	
CC(5): customer data	External unauthenticated partner	None	
CC(6): customer data	External unauthenticated partner	None	
CC(7): customer data	Internal network partner	None	

The adherence of the security objective availability is evaluated with the values level and implemented countermeasures. The level specifies the frequency of meeting the

defined availability security objective and implemented countermeasures specifies different availability concepts. The two systems customer and credit card database used in the order process were rated as follows:

Table 3. Rating of availability of the systems used in the process

Availability	Level	Measure
A (1): Customer data (customer database)	always met	hot standby
A (2): Payment data (credit card database)	partially not met	hot standby

The adherence of the security objectives integrity and confidentiality for the data entities is determined by a criteria table applied to every assessed entry- (EP), process point (PP) and communication channel (CC) in table 2. The rules of the criteria table were developed on basis of the security objectives definition e.g. the confidentiality restriction to single users, company dependent definitions e.g. an internal network partner is trustworthy and dependencies between categories e.g. changes to data must be validated to be accurate or complete. An example for a rule is: The security objective integrity rated as poor is only adhered to when the ratings for every EP and PP for the basic concepts access control, authorization and data validation have a certain level of rating. Because of space limitations we have not included the criteria table used for the rating of integrity, confidentiality and availability. The rules can be represented as facts in Prolog. We have implemented the validation rules of the criteria table in Prolog to support the analysis.
The assessment of the security requirements is currently rated with a simple value "security level" for each EP, PP and CC to determine whether the technical implementation of the measures access control, authorization, data validation and communication/encryption complies with current best practices. In the future we will specify in detail the data security requirements regarding confidentiality, integrity and availability. The overall assessment (security objectives and requirements) of a data entity concerning all EP, PP and CC is a consolidation of the security objectives and the security requirements rating. All data entities (1-x) have to be checked whether the security objectives integrity, confidentiality, availability or the security requirements for an EP(1-x), PP(1-x) or CC(1-x) are not adhered to. If there is any rating with failed then the security objective is not adhered to. The overall rating for the order process is:

Table 3. Overall rating for the order process of the single data units

Data entity	Sec. objective	Rating	Overall assessment
Customer data	integrity	average	failed
Customer data	confidentiality	Internal	failed
Customer data.	availability	1 business day	ok
Payment data	integrity	average	failed
Payment data	confidentiality	confidential	failed
Payment data	availability	24 hours	ok

The assessment of the security objectives on a data entity level reveals IT risks to the company as the data is the core element of all business transactions. In our example the results show that integrity and confidentiality of customer and payment data are at risk as the security objectives or requirements are not adhered to. An analysis of the single data process points of the business process and their ratings shows definitely where the reason is for non-adherence. In our example the principal reason for non-adherence is the missing encryption of customer and payment data.

3. Critical discussion of the approach

With the proposed method IT security risks within an organization arising from non-adherence of security objectives and security requirements can be determined as well as current threats to systems. It is our expectation that, compared with existing approaches in practice, the approach will provide comparatively reliable and detailed results under the tight time constraints given in practice. The main advantages of the approach are:

- the assessment is conducted on reliable and readily available data (business process models) and does not need any re-engineering of processes,
- the approach does not need any probability statistics or estimations and checks current system implementations
- it is focused on critical processes and assets for business operation,
- it considers security requirements, current countermeasures and system implementations as well as organizational issues.

Therefore we expect that the approach will be more time efficient, easier to handle and more accurate than traditional approaches. An empirical validation of this assumption is planned for future work (e.g. by extending existing results such as [25]).

There are, however, some concerns with the current state of the proposed approach, which we intend to improve on in future work:

- The evaluation rules for integrity and confidentiality were created on security objectives and company specific rules (e.g. trustworthiness of an internal network partner). We will need to further validate the rule base and separate more precisely between security objective and company specific rules.
- Access control, authorization, data validation and communication were chosen as assessment criteria with different graded values. The employed categories and criteria are basic security concepts and classifications of the IT security domain but will need to be further validated.
- The assessment of the EP, PP and CC is currently conducted by a security expert and therefore not automated and objective. In addition the assessment of the security requirements might be hard but could probably be linked with other assessment approaches or best practices such as ISO27001 or HAZOP.
- The security requirements are currently rated at a qualitative level and not further specified. Therefore the high-level evaluation is still somewhat imprecise as well as dependent on the security expert knowledge.

Further work on the assessment approach will focus on the detailed security requirements specification in the definition stage as well as validation issues. For the security requirements we will substantiate the attributes for evaluation as well the dependencies between security objectives and used security concepts. Furthermore we intend to validate our approach with various audits in subsidiaries, business client assessments and a comparison with traditional approaches. For this it is planned to assess security risks first with the proposed approach and then to audit the subsidiary independently of the results with a traditional approach and afterwards compare both results regarding consistency and reliability. Secondly the proposed approach might be used to evaluate the insurability of business interruption at clients. For this we might use the assessment results (positive and negative ones) and the loss history to evaluate the accuracy. In addition we intend to verify our results with occurred security incidents to check how accurate the results are regarding the system affected and type of incident. Furthermore we plan to extend the approach to evaluate the adherence to compliance requirements as well as to take into account the IS process maturity assessment.

References

1. M. Backes, B. Pfitzmann, and M. Waidner, “Security in Business Process Engineering,” W. van der Aalst, A. ter Hofstede, and M. Weske (Eds.): BPM 2003 , Springer Publishing, 2003, P. 168-183.
2. K. Badenhorst and J. Eloff, “TOPM: a formal approach to the optimization of information technology risk management,” Computers & Security, vol. 13, 1994, P. 411-435.
3. J. Brodkin, “TJX breach may spur greater adoption of credit card security standards,” Networkworld, March 2007; http://www.networkworld.com/news/2007/032907-tjx-breach-adopt-standards.html .
4. M. Gerber and R. von Solms, “From Risk Analysis to Security Requirements,” Computers & Security, vol. 20, 2002, P. 577-584.
5. S. Halliday, K. Badenhorst and R. von Solms, “A business approach to effective information technology risk analysis and management“ Information Management&Computer Security, vol. 4/1, 1996, P. 19–31.
6. D. Hartnett , “Text of letter on benefit records loss,” British Broadcasting Corporation (BBC), Nov. 2007; http://news.bbc.co.uk/1/hi/uk_politics/7107853.stm.
7. P. Herrmann and G. Herrmann, “Security requirement analysis of business processes,” Electron Commerce Research, vol. 6, 2006, P. 305- 335.
8. G. Herrmann and G. Pernul, “Towards Security Semantics in Workflow Management,” Proceedings of the 31st Annual Hawaii International Conference on System Sciences (HICSS-31), IEEE : 1998.
9. J. Hitchings, “Achieving an integrated design: the way forward for information security,” in Ellof, J. and von Solms, S. (Eds), Information Security: the Next Decade, IFIP SEC 1995.
10. R. Holbein, S. Teufel and K. Bauknecht, “The use of business process models for security design in organisations,” in Katsikas, S. and Gritzalis, D. (Eds), IFIP SEC 1996.
11. P. Hosking, C. Bremner and A. Sage, “Jerome Kerviel named in €5bn bank trading fraud,” TimesOnline, Jan. 2008; http://business.timesonline.co.uk/tol/business/industry_sectors/banking_and_finance/article3242996.ece.
12. S. H. Houmb, G. Georg, R.B. France, J.M. Bieman, J. Jürjens: Cost-Benefit Trade-Off Analysis Using BBN for Aspect-Oriented Risk-Driven Development. ICECCS 2005: p. 195-204.
13. S. Kaplan, “The Words of Risk Analysis,” Risk Analysis, vol. 17, 1997.
14. S. Kokolakis, A. Demopoulos and E. Kiountouzis, “The use of business process modeling in information systems security analysis and design,” Inf.Manag.&Comp. Security, 8, 2000, p. 107-116.
15. M. Martin and J. Dobson, “Enterprise modelling and security policies,” in Jajodia, S. and Landwehr, C.E. (Eds), Database Security IV: Status and Prospects, Holland: Elsevier Science Publ., 1991.
16. T. Neubauer, M. Klemen and S. Biffl, “Business Process-based Valuation of IT-Security,” EDSER'05, St. Louis, Missouri, USA: ACM, 2005.
17. R.K. Rainer, C.A. Snyder and H.H. Carr, “Risk Analysis for Information Technology,” Journal of Management Information Systems, vol. 8, 1991, P. 129-147.
18. C. Ribeiro and P. Guedes, “Verifying Workflow Processes against Organization Security Policies,” 8th IEEE International Workshops on Enabling Technologies, 1999, P. 190-191.
19. A. Rodriguez, E. Fernandez-Medina and M. Piattini, “A BPMN Extension for the Modeling of Security Requirements in Business Processes,” IEICE Trans. INF. & SYST., vol. E90–D, Apr. 2007.
20. S. Roehrig and K. Knorr, “Security Analysis of Electronic Business Processes,” Electronic Commerce Research, vol. 4, 2004, P. 59-81.
21. A. Stewart, “On risk: perception and direction,” Computers&Security, vol. 23, 2004, P. 362-370.
22. B. Suh und I. Han, “The IS risk analysis based on a business model,” Information & Management, vol. 41, 2003, P. 149–158.
23. W. Thoben, “Wissensbasierte Bedrohungs-und Risikoanalyse Workflow-basierter Anwendungs-systeme“, Reihe Wirtschaftsinformatik, B.G. Teubner-Verlag, Stuttgart 2000
24. M. zur Muehlen, “Integrating Risks in Business Process Models,” 16th Australasian Conference on Information Systems, Sydney: 2005.
25. K. Buyens, B. De Win, W. Joosen: Empirical and statistical analysis of risk analysis-driven techniques for threat management. ARES 2007: 1034-1041
26. J. Jürjens, Secure Systems Development with UML, Springer 2004
27. M. Alam, M. Hafner, and R. Breu, “Model-Driven Security Engineering for Trust Management in SECTET”, Journal of Software 2/1, Feb 2007
28. J. Whittle, D. Wijesekera, M. Hartong: Executable misuse cases for modeling security concerns. ICSE 2008: 121-130
29. S.T. Redwine, “Introduction to Modeling Tools for Software Security”, Build Security In body of knowledge, 2007
30. H. Mouratidis, J. Jürjens, J. Fox: Towards a Comprehensive Framework for Secure Systems Development. CAiSE 2006: 48-62
31. C.B. Haley, R.C. Laney, J.D. Moffett, B. Nuseibeh: Security Requirements Engineering: A Framework for Representation and Analysis. IEEE Trans. Software Eng. 34(1): 133-153 (2008)