A Survey of Scientific Approaches Considering the Integration of Security and Risk Aspects into Business Process Management

Stefan Jakoubi[1], Simon Tjoa[1], Gernot Goluch[1], Gerald Quirchmayr[2, 3]
[1]Secure Business Austria
{sjakoubi, stjoa, ggoluch}@securityresearch.at
[2]University of Vienna, [3]University of South Australia
gerald.quirchmayr@{[2]univie.ac.at, [3]unisa.edu.au}

Abstract

In the past years, regulative bodies have obliged a more stringent consideration of risk and security management. This development forced companies to apply risk, security and business process management in a more integrated way. Simultaneously, it can be observed that the scientific community intensified research activities in this integrative domain. Within this survey paper we examine scientific research efforts in the field of security and risk related business process/workflow management. Therefore we survey nine representative approaches and identify research challenges in this area.

1. Introduction

The basis for any improvements to stay competitive is a company's capability to execute its business processes correctly and continuously. Following Gartner's CIO report [1] improving business process is the most important business priority in the year 2009. Additionally, within the last years, the private sector has noticed a growing need to improve security to meet tighter regulative and legal requirements.

The major goal of this paper is to provide an overview of scientific research efforts regarding the integration of security as well as risk considerations into business process management. Furthermore, we want to motivate researchers by highlighting relevant and still open research challenges.

This rest of the paper is structured as follows: Chapter 2 gives an overview about approaches aiming at the integration of security and risk into business process management. Due to space limitations, we decided to concentrate on nine representative and different approaches in order to substantiate the identified open research challenges discussed in chapter 3.

2. Scientific Approaches and Results

This section is dedicated to the description of selected approaches and methods. It should serve as a starting point for the discussion of open research topics.

2.1 Process Oriented Security Model (POSeM)

The POSeM approach [2] has the objective to facilitate the selection process of security measures by providing recommendations derived from process descriptions. The two main concepts to meet this objective are (1) its Security Enhanced Process Language (SEPL) which enables the representation of security requirements within business processes and (2) two rule bases in order to check the process security definitions for consistency and afterwards identify required safeguards.

POSeM consists of four to five steps (outlined in Figure 1), which are described in the following paragraphs.

1. Definition of general security objectives: Before the analysis the general objectives have to be defined. This includes the definition of business aims as well as security objectives.
2. SEPL: Security Enhanced Process Language: Values for security objectives are assigned to each business process components (i.e. actors, artifacts and activities).
3. Consistency analysis: The first rule base is applied in order to perform consistency checks. If one of the checks fails, the SEPL model has to be revised.
4. Derivation of generic security measures: Security measures are derived on the basis of the SEPL description using the second rule base.
5. Implementation: The identified (generic) security measures are mapped to security measures of real systems. This is not an integral part of the POSeM method".

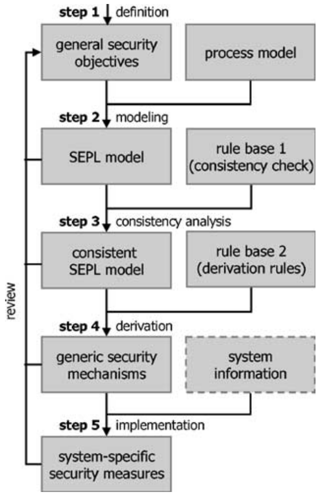


Figure 1 Steps of the POSeM Approach [2]

2.2 Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes

The major contribution of the authors' work is an extension of UML 2.0 in order to enable the definition of business analysts' security requirements into business processes [3]. According to the authors, this is essential since software developers derive necessary requirements for software design and implementation from business processes. This early design of security requirements shall (1) use the (at least high-level) security knowledge of business analysts concerning business process security while initially modeling the processes and (2) reduce potential costs avoiding the additional implementation of business processes' security after the business processes have been implemented. "Moreover, capturing the security requirements of a system is a hard task that must be established at the initial stages of system development, and business processes offer a view of business structure that is very suitable as a basis for the elicitation and specification of security requirements" [3].

The authors refer to related work which discusses the use or extension of UML diagrams for capturing security requirements. However, according to the authors, the related work considered does not concentrate on the use of activity diagrams.

The proposed extensions (as shown in Figure 2) aim on allowing business analysts to define security requirements of business processes using activity diagrams. These security requirements have later to be completed by security analysts.

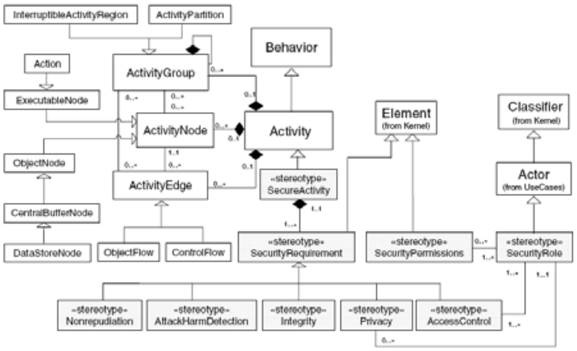


Figure 2 Proposed UML 2.0 Extensions [3]

2.3 Process Mining and Security: Detecting Anomalous Process Executions and Checking Process Conformance

The major contribution is the use of process mining in order to infer Petri-net based workflow representations from systems' event logs through applying the α-algorithm. This enables the authors' approach [4] to (1) check the validity/conformity of new event log entries and (2) to check the conformity of event log entries regarding modeled security related patterns (e.g. activity "provide password" must be executed in advance of "process order").

The authors define two conditions in order to be able to apply their approach: (1) the event log must contain sufficient information and (2) the inferred Petri-net must satisfy certain requirements so that they represent Structured Workflow Nets". According to the authors, these requirements have to be met in order to enable the application of the proposed mining algorithms.

The authors distinguish three mining perspectives (see also Figure 3):

- The process perspective focuses on the control-flow (the "how?"). Mining goal: Determining a "good characterization of all possible paths".
- The organizational perspective focuses on the originator field (the "who?"). Mining goal: Structuring the organization and showing relations between individual performers.
- The case perspective focuses on properties of cases. "Cases can be characterized by their path in the process or by the originators working on a case" (the "what?").

Once the net is discovered, two checks are possible: (1) checking of every new audit trail; (2) checking of process conformance.

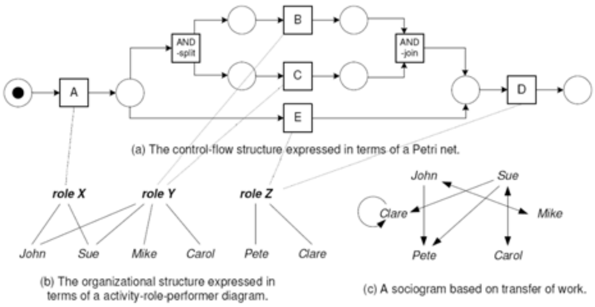

A
AND -split
B
C
E
AND -join
D
(a) The control-flow structure expressed in terms of a Petri net.
role X
role Y
role Z
John
Sue
Mike
Carol
Pete
Clare
(b) The organizational structure expressed in terms of a activity-role-performer diagram.
John
Sue
Clare
Mike
Pete
Carol
(c) A sociogram based on transfer of work.

Figure 3 Mining results for the process perspective (a) organizational (b) (c) perspective based on event log [4]

2.4 Integrating Risks in Business Process Models

Zur Muehlen and Rosemann tackle the topic of risk-oriented process management [5]. The authors identify risk as an inherent property of every business process. To counteract the trend of considering risk only from a project management viewpoint they address the topic of risk management in the context of business process management. Therefore they introduce and discuss a taxonomy (depicted in Figure 4) of process related risks and its possible applications in the field of analysis and documentation of business processes. Furthermore, a taxonomy for business processes is presented, including five clusters (goals, structure, information technology, data and organization) and two distinguished lifecycles (build-time and run-time), enabling the classification of both errors and risk. Moreover four interrelated model types are presented to capture risk in the context of business processes: (1) Risk Structure model, providing insights into the relationship between risks. (2) Risk Goal model, depicted by a risk/goal matrix. (3) Risk State model, capturing the dynamic aspects of risk and consisting of the object types risk, consequence and connectors (XOR and AND). (4) EPCs (Event-driven Process Chain) extended with risks, enabling the assignment of risks to individual steps in the process.

2.5 Integrating Risks in Business Process Models with Value Focused Process Engineering

Neiger et al. focus their work on the need for a holistic business view on risk management in the enterprise systems space [6]. The foundation for this holistic view is value-focused process engineering which can be described as follows: "Value-focused process engineering creates links between business processes and business objectives at the operational and strategic levels" [6]. The introduced framework applies the abovementioned value-focused process engineering principles to risk management models leading to risk-oriented process management and consists of the following four steps: (1) Business values and objectives are decomposed to identify relevant process risks, while each business activity is examined in order to identify further relevant risks. (2) Value-focused approaches are used to identify specific risks and to determine the processes and corresponding functions which contribute to these risks. (3) Process configurations are proposed to identify the best process structure that meets the business objectives. (4) The comparison of alternative configurations and their corresponding results finally enables the choice of the optimal process configuration that meets the identified risk minimization objectives, with regards to overall business requirements. Figure 5 schematically outlines the described four step process using EPC-notation.

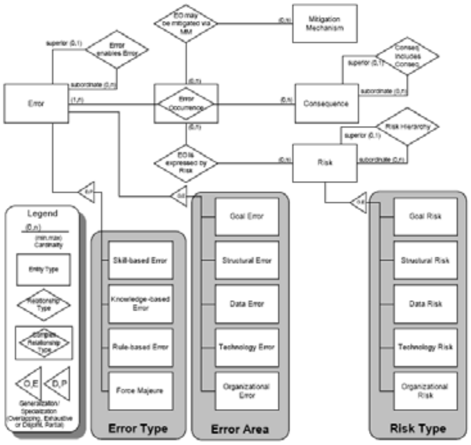


Figure 4 Risk Taxonomy [5]

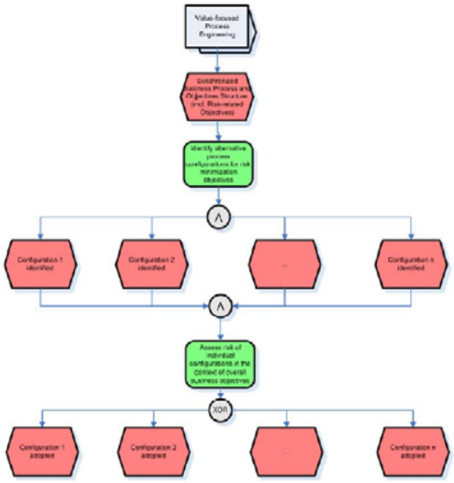

Value-focused Process Engineering
Synchronized Business Process and Objectives Structure (incl. Risk-related Objectives)
Identify alternative process configurations for risk minimization objectives
Λ
Configuration 1 identified
Configuration 2 identified
...
Configuration n identified
Λ
Assess risk of individual configurations in the context of overall business objectives
XOR
Configuration 1 adopted
Configuration 2 adopted
...
Configuration n adopted

Figure 5 Process management and risk assessment linking process [6]

2.6 Modeling Business Process Availability

Milanovic et al. present a framework for modeling business process availability taking services, underlying ICT infrastructure and human resources into account [7]. The authors adapted a service-enabled architecture to model the abovementioned relations. Figure 6 outlines the proposed architecture. Furthermore, the framework uses a fault-model with two failure modes (Temporal: service/business process does not meet deadline. Value: service/business process responds with incorrect value or performs incorrect function) for its analytical assessment procedure that consists of the following seven steps: (1) Describing the business process using a process modeling language; (2) Refining activities by modeling atomic services with the same formalism; (3) Creating an infrastructure graph; (4) Services mapping to the infrastructure components and paths for service executions are transformed into Boolean expressions; (5) Business processes mapping with atomic services leading to Boolean equations that express the functional dependency between business process, service and ICT-layer availability; (6) Transforming the Boolean expressions into reliability block diagrams/fault trees to calculate steady-state availability; (7) Calculating the availability of business process and services by solving/simulating the model generated within the abovementioned steps.

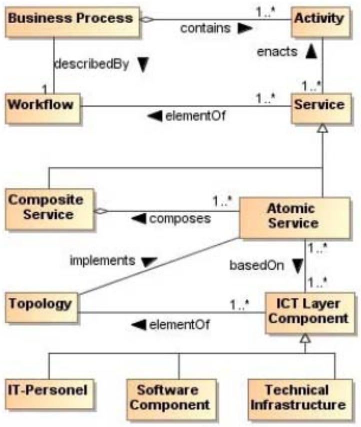


Figure 6 Service-enabled Architecture [7]

2.7 IT Risk Reference Model

Sackmann extends current risk management methods with a business process-oriented view leading to an IT risk reference model (see Figure 7) which builds the bridge between the economic and more technical layers including vulnerabilities [8] [9]. The introduced model consists of four interconnected layers: (1) Business process layer; (2) IT applications / IT infrastructure layer; (3) Vulnerabilities layer; (4) Threats layer. This reference model "serves as foundation for formal modeling of the relations between causes of IT risks and their effects on business processes or a company's returns" [8]. For expressing these relations (i.e. the searched cause-effect relations) a matrix-based description is used.

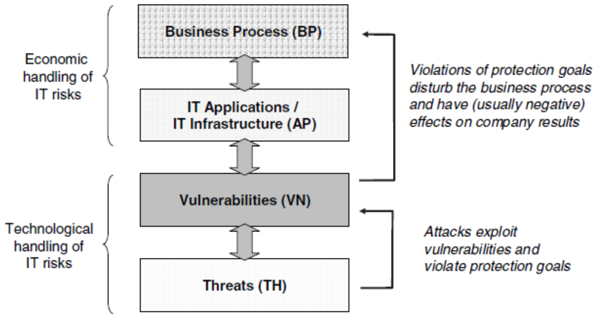

Economic handling of IT risks
Business Process (BP)
IT Applications / IT Infrastructure (AP)
Vulnerabilities (VN)
Threats (TH)
Technological handling of IT risks
Violations of protection goals disturb the business process and have (usually negative) effects on company results
Attacks exploit vulnerabilities and violate protection goals

Figure 7 Risk Reference Model [8]

2.8 Risk-Oriented Business Process Evaluation (ROPE)

The ROPE (Risk-Oriented Process Evaluation) methodology focuses on the simulation-based evaluation of threats' impact on the execution of business processes [10] [11]. Therefore, the basic concept is as follows: Business process activities require resources in order to be adequately executed. Occurred threats impact the functionally of resources until – if not appropriately defeated – one or more affected resources are not available any more. In the worst case a resource represents a single point of failure and consequently hinders the execution of the related business process activity. Besides the business processes, counter and recovery measure processes are modeled. In the case that a threat is detected, the appropriate counter measure process is invoked counteracting the threat. If the threat could be defeated, recovery processes are invoked in order to re-establish the functionality of the affected resource until it is again available for the respective business process activity.

ROPE consists of three modeling layers enabling the so called risk-aware business process modeling and simulation. (1) Within the process layer, business as well as counter and recovery measure process activities are modeled. (2) Resources within the resource layer are allocated to one or more business process activities and are modeled in a tree-based structure. Furthermore, the resources are interconnected with the logical operators AND and OR (in order to enable the modeling of redundancies). (3) Within the threat/impact layer identified threats are modeled and assigned to resources.

Simulating the whole model on the one hand enables the determination of business processes' delays in the case of occurred threats considering implemented counter and recovery measures (see Figure 8). On the other hand, it is possible to determine additional times and costs (of activities and required resources) when invoking counter and recovery measure processes. Manifold different scenarios can be modeled enabling simulation-based identification of a company's critical business processes and single points of failure.

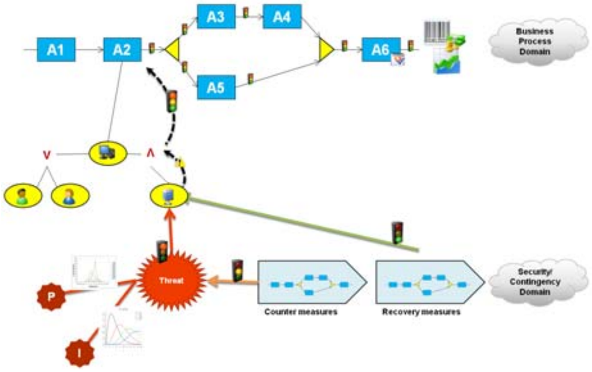


Figure 8 Overview: Risk-Aware Business Process Modeling and Simulation

2.9 Business Process-based Valuation of IT-Security

Neubauer et al. propose an IT-Security Valuation Framework which aims at establishing the connection between a company's core business processes, IT-processes and security levels [12]. Figure 9 provides an overview about the framework. Core business processes are used to determine the external value regarding the valuation of security measures. This valuation bases on the determination of downtime costs (lost business value) in the case of a system's unavailability. IT processes are used to measure "the costs needed for implementing and keeping a defined level of security" (e.g. investment, operation or recovery costs). On the basis of the information gained from the analysis of the core business processes and IT processes valuation models such as ALE (Annual Loss Expectancy) can be used for calculating the expected loss and defining the optimal level of security.

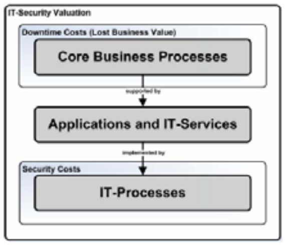


Figure 9 IT-Security valuation based on Core Business Processes and IT-Processes [12]

4. Discussion and Conclusion

The domain of business process security is still a very young research domain compared to the business process domain. Within this survey paper we have summarized a variety of approaches trying to diminish the gap between business process management, security and the risk management domain.

Within this paper we provided a representative overview of the efforts in this field and finally, we have come to the conclusion that this emerging field of research still has a lot of potential, if certain challenges can be solved.

In the following we categorize the introduced approaches in order to give a starting point for researchers interested in the domain of business process security and furthermore, highlight the different characteristics and priorities of each approach according to the succeeding criteria:

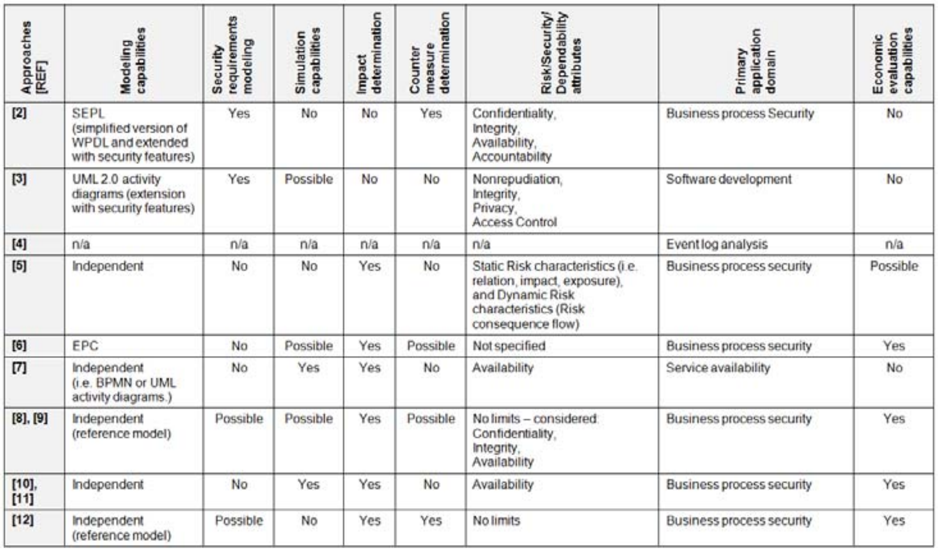
(1) **Modeling capabilities:** Indicates which modeling languages are supported; (2) **Security requirements modeling:** This criterion provides information which and how security requirements can be modeled within the approach; (3) **Simulation capabilities:** Within this category it is examined whether an approach supports simulation; (4) **Impact determination:** Within this aspect it is surveyed which kind of impacts (e.g. financial, reputational, operational …) is supported by the approach; (5) **Counter measure determination:** This part outlines whether it is possible to derive counter measures when using the approach; (6) **Risk/Security/Dependability attributes:** Examines which attributes are considered by the approach (e.g. risk, confidentiality, integrity, availability, safety …); (7) **Application domain:** Outlines whether the approach is domain independent or tailored to a specific domain (e.g. software domain) ; (8) **Economic evaluation capabilities:** This criteria illustrates whether cost benefit evaluation of counter measures are supported.

The results of the evaluation are presented in table 1. The evaluation serves as input to identify promising research areas in the field of business process security. For clarity, approach [4] does not fit in the comparison. However, as it delivers substantial research results in the area of business process security we did not want to lose this research work.

From our perspective, the succeeding listing illustrates challenges, derived by this survey, which should be rigorously addressed to build the comprehensive bridge between the business process and security/risk domains.

- Consideration of different impact perspectives (e.g. reputation, financial, operational, etc.)

Table 1 Comparison of Business Process Security Approaches



Approaches [REF]	Modeling capabilities	Security requirements modeling	Simulation capabilities	Impact determination	Counter measure determination	Risk/Security/ Dependability attributes	Primary application domain	Economic evaluation capabilities
[2]	SEPL (simplified version of WPDL and extended with security features)	Yes	No	No	Yes	Confidentiality, Integrity, Availability, Accountability	Business process Security	No
[3]	UML 2.0 activity diagrams (extension with security features)	Yes	Possible	No	No	Nonrepudiation, Integrity, Privacy, Access Control	Software development	No
[4]	n/a	n/a	n/a	n/a	n/a	n/a	Event log analysis	n/a
[5]	Independent	No	No	Yes	No	Static Risk characteristics (i.e. relation, impact, exposure), and Dynamic Risk characteristics (Risk consequence flow)	Business process security	Possible
[6]	EPC	No	Possible	Yes	Possible	Not specified	Business process security	Yes
[7]	Independent (i.e. BPMN or UML activity diagrams.)	No	Yes	Yes	No	Availability	Service availability	No
[8], [9]	Independent (reference model)	Possible	Possible	Yes	Possible	No limits – considered: Confidentiality, Integrity, Availability	Business process security	Yes
[10], [11]	Independent	No	Yes	Yes	No	Availability	Business process security	Yes
[12]	Independent (reference model)	Possible	No	Yes	Yes	No limits	Business process security	Yes

- Occurrence probabilities of threats
- Extension of security/dependability attributes (availability, confidentiality, integrity, accountability, safety etc.)
- Efficient resource allocation taking security aspects into account
- Improvements on the current business process notations to facilitate risk/security evaluation
- Providing metrics on the security and robustness of business processes

We are convinced that solutions regarding these challenges deliver enormous value leading to enhanced and more justifiable security investment decisions and significant improvements in organizational resilience.

5. References

[1] Gartner Inc., Gartner EXP Worldwide Survey of More than 1.500 CIOs Shows IT Spending to Be Flat in 2009, Available at http://www.gartner.com/it/page.jsp?id=855612, Accessed April 2009.

[2] S. Röhrig, Using Process Models to Analyse IT Security Requirements, Phd. Thesis, University of Zurich, 2003.

[3] A. Rodríguez, E. Fernández-Medina, M. Piattini, Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes, In: Proceedings of Trust and Privacy in Digital Business (TrustBus 2006), Springer, 2006.

[4] W.M.P. van der Aalst, A.K.A. de Medeiros, Process Mining and Security: Detecting Anomalous Process Executions and Checking Process Conformance, In N. Busi, R. Gorrieri, and F. Martinelli, editors, Second International Workshop on Security Issues with Petri Nets and other Computational Models (WISP 2004), STAR, Servizio Tipografico Area della Ricerca, CNR Pisa, Italy, 2004.

[5] M. zur Muehlen, M. Rosemann, Integrating Risks in Business Process Models, In proceedings of the 2005 Australasian Conference on Information Systems (ACIS 2005), Manly, Sydney, Australia, 2005.

[6] D. Neiger, L. Churilov, M. zur Muehlen, M. Rosemann, Integrating Risks in Business Process Models with Value Focused Process Engineering, In proceedings of the 2006 European Conference on Information Systems (ECIS 2006), Goteborg, Sweden, 2006.

[7] N. Milanovic, B. Milic, M. Malek, Modeling Business Process Availability, In Proceedings of the IEEE International Conference on Services Computing (SCC 2008), Honolulu, Hawaii, USA, 2008.

[8] S. Sackmann, A Reference Model for Process-oriented IT Risk Management, in: Golden, W. et al. (Eds.): 16th European Conference on Information Systems (ECIS'08), Galway, Ireland, 2008

[9] S. Sackmann, L. Lowis, K. Kittel, Selecting Services in Business Process Execution – A Risk-based Approach, in: H.R. Hansen et al. (Eds.), Business Services: Konzepte, Technologien, Anwendungen, Tagung Wirtschaftsinformatik (WI'09), Vienna, 2009

[10] S. Jakoubi, G. Goluch, S. Tjoa, G. Quirchmayr, Deriving Resource Requirements Applying Risk-Aware Business Process Modeling and Simulation, Proceedings of the 16th European Conference on Information Systems (ECIS 2008), 2008.

[11] S. Tjoa, S. Jakoubi, G. Quirchmayr, Enhancing Business Impact Analysis and Risk Assessment applying a Risk-Aware Business Process Modeling and Simulation Methodology, Proceedings of the 3rd International Conference on Availability, Reliability and Security (AReS 2008), IEEE, 2008.

[12] T. Neubauer, M. Klemen, S. Biffl, Business Process-Based Valuation of IT-Security, In Proceedings of the seventh international workshop on Economics-driven software engineering research (EDSER 2005), St. Louis, Missouri, USA, 2005.