A Reference Model for Risk-Aware Business Process Management

Stefan Jakoubi, Simon Tjoa
Secure Business Austria
{sjakoubi, stjoa}@securityresearch.at

Abstract

The major contribution of this paper is the introduction of a reference model which is capable to consider information acquired within the business process management and risk management domain. The central objective of the reference model is to enable the modeling of risk aspects in such a way that it provides the foundation for risk-aware business process simulations.

Within this paper, we firstly present an approach that combines essential activities of business process and risk management leading to risk aware business process management within an organization. Secondly, we illustrate our novel reference model which comprises extensions of existing modeling languages in order to meet our simulation-based risk-evaluation needs. We conclude this paper stating future research challenges.

Keywords: Business Process Management, Risk Management, Security Enablement Methods and Tools, Reference Model.

1. Introduction

In today's economy, risk management and business process management play a prominent role. The continuous improvement of economic aspects of a company's business processes is the foundation to stay competitive. Thus it is no big surprise that Gartner [16] states the improvement of business processes in its CIO report as number one priority. The research effort that has been performed for years in the field of modeling and optimizing processes from an economic viewpoint highlights the importance of business process management as well.

Exemplarily, approaches such as the Business Process Management Systems (BPMS) Paradigm [24] and Event-Driven Process Chains (EPC) [21] are used to model business processes and to optimize them regarding the effective and efficient use of resources.

Apart from the economic requirements, one could recently observe that due to regulatory and legal requirements, such as the Sarbanes Oxley Act (SOX) [28] or the EU audit directives [29] more and more business process management approaches try to integrate compliance aspects. Most approaches treating compliance issues introduce the ability to model control objects in order to check compliance. When we take a closer look to information security one can see that the integration of risk management would be the next logical step.

Risk management is mainly considered separately from business process management although large parts, such as understanding the business environment within the organization operates, overlap. A company's processes constitute the basis for risk management as risks always ultimately affect the business. Furthermore, faster changes of market conditions, dynamic business processes as well as the growing dependency on outsourced services require the stronger interweaving of both, the business process management and the risk management domain. There exist some research papers and approaches (e.g. [30]) on how risks can be modeled using extensions of various notations such as the ADONIS® standard modeling language [23], EPC [22], BPMN [19] or UML [20]. However, only limited research can be found that tries to use simulation-based risk evaluation of business processes. A detailed survey covering current research efforts in the field of business process security can be found in [11].

The major contribution of this work is the introduction of a novel reference model enabling risk-aware business process management. This reference model paves the way for risk aware business process simulations.

The term *risk aware business process management* is understood as the integration of a risk perspective into business process management. We therefore propose a set of extensions required for the business process and risk management domain in order to consider risks in business processes in an integrated way. For clarity, we use the term *risk* according to [12], [18] as the "combination of the probability of an event and its consequences".

The rest of this paper is organized as follows: Section 2 briefly presents three representative approaches showing current research efforts within the field of business process security. Section 3 outlines which activities are required to apply our risk-aware business process management approach. Section 4 introduces the extensions needed to fulfill risk-aware business process modeling and simulation according to [6], [7], [8], [9], [10]. We conclude our paper in Section 5 and sketch future research steps.

2. Related Research

In the following paragraphs we describe three representative research approaches of the last years which aim at the integration of risk aspects into economic business analyses. This selection comprises a proposed reference model and extensions of modeling languages and thus shall give an impression about addressed areas. For interested readers, we kindly refer to the outlined further relevant related research [11].

Sackmann extends current risk management methods with a business process-oriented view leading to an IT risk reference model which builds the bridge between the economic and more technical layers including vulnerabilities [1], [2]. The introduced model consists of four interconnected layers: (1) Business process layer: A business process consists of activities and sub-processes. To quantify IT risks, it is necessary that the monetary value of the process for the company can be calculated. (2) IT applications / IT infrastructure layer: this layer comprises all required IT applications and underlying infrastructure components. (3) Vulnerabilities layer: the layer includes "… all vulnerabilities that exist in the components…" [1] of the IT applications / IT infrastructure layer. (4) Threats layer: this layer comprises all threats that can result in IT risks. Ideally, the occurrence probability should be determined. 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" [1]. For expressing these relations (i.e. the searched cause-effect relations) a matrix-based description is used.

CORAS [3] is a method for conducting security risk analysis, which is abbreviated to "security analysis". CORAS provides a customized language for threat and risk modeling, and comes with detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis. The Unified Modeling Language (UML) is used to model the target of the analysis. For documenting intermediate results and for presenting the overall conclusions special CORAS diagrams which are inspired by UML are used. The CORAS approach comprises the succeeding seven steps. (1) Introductory meeting: Information gathering is performed through an introductory meeting. The representatives of the client present their goals of the analysis and the target to be analyzed. (2) High-level analysis: Separate meetings with the representatives where the analysts present their understanding of what they learned at the first meeting and from studying documentation which have been provided by the client. The meeting includes a first high-level security analysis where threats, vulnerabilities, threat scenarios and unwanted incidents are identified. This input is used to direct and scope the further detailed analysis. (3) Approval: Refining the description of the target to be analyzed and identifying all assumptions and other preconditions being made. (4) Risk identification: Through a workshop with experienced people as many potential unwanted incidents, threats, vulnerabilities and threat scenarios as possible are identified. (5) Risk estimation: Through a workshop estimates on consequences and likelihoods of unwanted incidents are identified. (6) Risk evaluation: Presenting the client the first overall risk picture. This typically triggers adjustments and corrections. (7) Risk treatment: Through a workshop treatment and cost / benefit issues are identified.

Karagiannis et al. [17] present in their work a business process oriented approach to support Sarbanes Oxley Act (SOX) compliance efforts of organizations. The authors propose a six step approach supported through the ADONIS® platform. Furthermore they extended the ADONIS® standard modeling language in order to meet the requirements demanded by SOX and COSO (Committee of Sponsoring Organizations). The six steps framework consists of the following phases: (1) Business Process Acquisition: Business processes serve as the foundation of the approach and are therefore acquired within the first step. (2) Risk Assessment and Scoping: In a second step SOX-related risks (including likelihood and impact) are identified and modeled. The relation between the risk and the concerned business process is also addressed. Moreover, controls are documented using a control model. (3) Design Effectiveness: This stage "… deals with the revision of internal controls, intended to balance risk and control costs …" [17]. (4) Operating Effectiveness: The aim of this step is the evaluation of the effectiveness of the current internal control set during operations. The authors propose self assessments, internal audit reviews or testing procedures as possible sources to determine the effectiveness. (5) Internal Management Review: This stage assesses predefined goals of the company against the test results of the previous steps to determine if the company is SOX-compliant. (6) Auditor's Final Review: Within the last step "… the external auditor receives financial reports along with internal management review reports …" [17]. The evaluation of this approach was performed at an US insurance company covering 180 business processes. Further details about the approach and the evaluation can be found at [17].

All mentioned approaches are substantial contributions in the field of business process security. However, to support our risk-aware business process management approach [6], [7], [8], [9], [10] we identified the following needs that could not be satisfied by the three representative approaches. (1) The reference model of Sackmann focuses on IT components and risks. For our model, we require a more comprehensive view comprising sufficient business process elements enabling a simulation (e.g. start, activity, decision elements) which can all be affected by risks. Furthermore, the resource model is not adequate for our simulation purposes as it is restricted to IT applications and their underlying infrastructure. Detection, counter and recovery measures are also not considered separately which is indispensible for our simulation approach. Without this separation it is hardly possible to conduct detailed evaluations of security settings.

The CORAS method includes risk-related information into UML diagrams for their security analysis purposes. However, the extensions are not sufficient to meet our modeling objectives. Furthermore, CORAS is not designed to perform simulations and concentrates on software security.

The ADONIS® platform used by the approach of Karagiannis et al. provides business process modeling and simulation capabilities. However, the introduced extensions to the business process meta-model focus on the integration of SOX compliance and respective controls. The extensions provide valuable information exemplarily for supporting audits and compliance management. However, the meta-model extensions are not sufficient to support all our requirements (e.g. consideration of dependability [31] attributes).

3. Risk-Aware Business Process Management

Within this section, we describe required phases for performing risk-aware business process management. The proposed phases must not be understood as rigid or inflexible but as requirements guidelines when setting up a respective program. The contents of these guidelines are essences from typical business process and risk management good practices such as [19], [24], [21], [25], [13]. However, we provide extensions (e.g. risk-aware business process simulation) in order to support risk-aware business process management. Further supportive project and business continuity management activities can be found in [26], [27], [4], [5], [14]. Figure 1 shows our proposed phases.

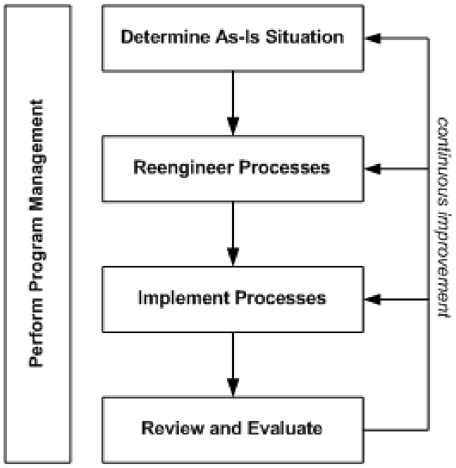

Figure 1. Required Phases for Performing Risk-Aware Business Process Management

Perform Program Management

Within the Program Management phase the fundamentals of the planned program are established. Therefore, at least the following major topics have to be addressed: (1) Scope, (2) Organizational Environment, (3) Evaluation Criteria, (4) Roles and Responsibilities, and (5) Program Steering.

The *Scope* of the program is essential to guarantee that the program achieves the expected objectives and results. It should be clearly defined what is inside and outside of the program. Typical content of the scope definition are the identification of included business units and core processes, the geographic scale as well as time and budget constraints.

The analysis of the *Organizational Environment* provides information of the overall strategic goals and the market in which the company currently operates or wants to operate (e.g. competitors, customers).

Evaluation Criteria must be measurable in order to be evaluated and to ensure the program's success. Economy related criteria exemplarily comprise a cost reduction of ten percent and security related criteria a service availability of at least 99 percent.

Roles and Responsibilities for the program planning, execution and controlling have to be defined. This exemplarily includes the establishment of a program coordination team comprising representatives of all required business units. Senior management buy-in is the basic prerequisite for the acceptance of the program.

The program coordination team is responsible for adequate *Program Steering*. This includes typical project management tasks such as time and budget management, quality management and program risk management.

Determine As-Is Situation

The main goal of this phase is to acquire sufficient information for succeeding analysis steps. Therefore, at least the following main tasks have to be performed: (1) Core Process Identification, (2) Resource Identification, (3) Risk Identification, and (4) Detection, Counter and Recovery Measure Identification.

Within the *Core Process Identification* involved business units have to be surveyed to gather sufficient information about core activities, possible execution paths and their probabilities. Furthermore, process (activity) characteristics such as execution times and costs as well as the value of the process (e.g. monetary value, intermediate products) have to be recorded.

Within the *Resource Identification* required resources, their interdependencies and their assignment to activities is determined. Additionally, resources which serve as input and are transformed into an output are identified.

The *Risk Identification* phase provides information on two types of risks: (a) *Business Risks* affecting process characteristics (e.g. change of invocation frequency, input parameters, change of decision probabilities) and (b) *Resource Risks* affecting dependability attributes such as confidentiality, integrity and availability (e.g. worm disrupting the functionality of servers).

The *Detection, Counter and Recovery Measure Identification* deliver information about implemented measures and processes. Detection measures (e.g. fire detectors) reduce the time period until implemented counter and recovery measures may be invoked. Preventive counter measures (e.g. non-smoking policy) reduce the occurrence probability. Reactive counter measures (e.g. fire sprinkler) decrease the potential impact. Recovery measures (e.g. restore of back-up tapes) re-establish the functionality of disrupted resources.

The acquired information is modeled according to the proposed reference model in section 4 to enable further analyses such as risk-aware business process simulations as introduced in [6], [7], [8], [9], [10].

Reengineer Processes

The Reengineer Processes phase aims at (re-) designing the company's business processes subsequent to the analysis of the gathered information. The driver of this phase is definitely the business. However, through risk-aware business process simulations the risk perspective is strongly integrated in the process improvement. The following phases have at least to be performed: (1) Business Impact Analysis, (2) Risk Analysis, (3) Identification of Improvement Options, (4) Redesign of Processes, and (5) Evaluation. As described in [6], [9], [10] our concept of risk-aware aware business process modeling and simulation can be applied to support these phases.

The *Business Impact Analysis* examines the impacts (e.g. financial, backlogs) of resources' and/or activities' disruptions over time (e.g. after one, two, eight hours, etc.). The main objective is to determine metrics such as the Maximum Tolerable Period of Disruption (MTPD) or the Recovery Point Objective (RPO). [15]

Within the *Risk Analysis*, identified risks and their impact on dependability attributes of resources and/or activities are considered. The main goal is to determine which risk should be addressed how (according to the company's risk strategy) and at which priority.

The result of the step *Identification of Improvement Options* is a set of improvement alternatives for economic as well as for security improvements. The options are presented to the senior management that has ultimately to decide what options should be applied.

Once it is decided which improvements should be implemented the *Redesign of Processes* is performed. Secure process structures and key controls (e.g. separation of duties) should be considered while modeling the processes.

The subsequent *Evaluation* guarantees that the redesigned processes meet the required objectives. Deficiencies identified within this step lead to a new iteration. The new iteration can start at each process of the *Reengineering Processes*. This assures the quality of the design and minimizes the threat of expensive design errors.

Implement Processes

The Implement Processes phase aims at realizing the designed processes. The steps necessary to apply new processes to an organization comprise at least the following: (1) Project Setup, (2) Implementation, and (3) Evaluation.

Within the *Project Setup* step implementation projects are set up. The roles and responsibilities for the projects are assigned and the cost and time constraints are defined.

The next step is the *Implementation* of the particular projects. Within the implementation it is important to evaluate specific technical solutions to realize the design and to introduce the new processes. It is essential for the success of the project that process changes within the organization are communicated clearly in order to improve acceptance.

The last step of this phase is the *Evaluation* of the implementation. If deficiencies are identified, the issues are documented and a new iteration can start either at the *Reengineer Processes* phase or at the *Implementation* step depending on the significance of the problem.

Review and Evaluate

As each organization is a living entity, processes and risks have to be periodically evaluated. This ensures that processes are improved on a regular basis and that changes in risk situation are promptly recognized. Furthermore, it is essential to test and exercise the security capabilities of an organization in order to build up an efficient and effective response for unwanted events. The stages that should be performed in this phase include: (1) Performance Review, (2) Risk Situation Review and (3) Security Plan Testing.

The *Performance Review* of the processes serves as a basis for continuous improvement. Therefore, this regular evaluation of performance, both from economic and security perspectives, is a central part of our proposed approach.

The *Risk Situation Review* deals with variations of risk factors as these can abruptly change. Also alterations in the environment (e.g. development of competitors, customer movements) and changes of the strategic alignment of an organization should be carefully reviewed within this phase. This is essential to stay competitive in today's economy.

The *Security Plan Testing* stage should ensure that all security-related plans (e.g. incident management plan, business continuity plan) are adequately tested. In order to enable continuous improvements in all described phases, iterations back to all previous phases (i.e. Determine As-Is Situation, Reengineer Processes, and Implement Processes) are possible.

Applying the above described phases enables risk-aware business process management. In the following section, we present our reference model.

4. The Reference Model

In this section, we firstly introduce our general reference model enabling risk-aware business process management. Secondly, we outline the minimal set of required business process and risk-related elements for our approach. We concentrate on this set in order to guarantee support for a broad range of modeling notations.

Figure 2 shows the general reference model enabling risk-aware business process management. Briefly, the fundamental concept is according to [6], [7], [8], [9], [10] as follows: Threats endanger certain business process elements (e.g. an activity or a resource). If a threat successfully attacks such an element, in the worst case the execution of the business process is interrupted or delayed. Detection measures influence the time period until when counter and recovery measures are invoked. Counter measures to mitigate a threat's impact and finally eliminate the threat. Recovery measures re-establish the execution of the business process (e.g. recovery of an affected resource).

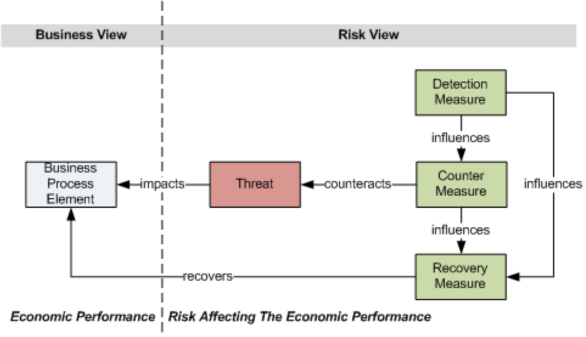

Figure 2. The General Reference Model

In order to enable risk-aware business process modeling, we introduce the succeeding risk-related elements:

A *Threat* occurs with a certain probability and affects business process elements with a certain impact.

A *Counter Measure* either reduces the occurrence probability of a Threat (i.e. preventive) or reduces the potential impact of an occurred Threat (i.e. reactive).

A *Recovery Measure* re-establishes the functionality of impacted resources and/or activities.

A *Detection Measures* influences the time periods until Counter and Recovery Measures are invoked.

Figure 3 schematically shows the minimal set of required business process elements. Below the figure, these elements are basically described including minimal required attributes.

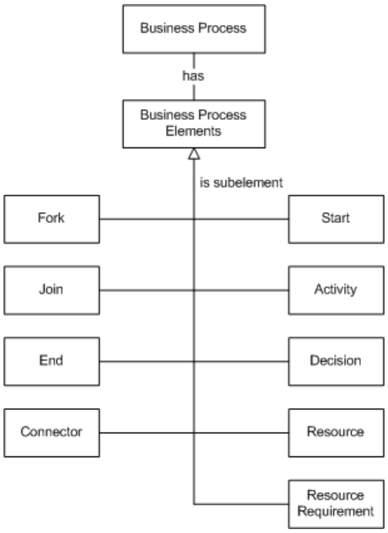

Figure 3. Minimal Set of Business Process Elements

Within our approach, a *Business Process* is the container for all further elements and consists of the succeeding *Business Process Elements*:

A *Connector* connects all Business Process Elements in order to describe the process flow.

A *Start* is the beginning of a Business Process. There can only be one Start element.

An *Activity* transforms an input using resources into an output. An Activity has at least the economic attributes *Execution Time* and *Costs*. For our purposes, an activity has the following further risk-related attributes: (1) a *Completion Function* which may be affected by an occurred threat; (2) the flag *Interruptible* that describes whether the execution of the activity may be delayed or the activity has to be totally re-executed; (3) Dependability Attributes (e.g. confidentiality, integrity, availability, etc.) stating the demand on the activity that it is correctly executed; (4) a *Priority* that serves in the context of all business process activities as decision support for recovery sequences.

A *Resource* is required by one or more Activities. A Resource has at least the economic attribute *Cost*. Furthermore, it has a *Type* (e.g. input or output) and *Dependability Requirements* stating the demand on the resource that it can be correctly used.

A *Resource Requirement* describes the interrelationship between an Activity and a set of Resources. The attribute *Dependability Level* states the demand of an Activity which has to be met by the resource (e.g. Resource A must be fully available). The attribute *Logical Connection* relates resources (e.g. logical operators AND or OR) in order to exemplarily represent redundancies.

A *Decision* splits the process flow into at least two branches. The attribute *Threshold* describes how branches are chosen. Typically, each branch has a certain probability that it will be chosen during a simulation. However, other constraints such as monetary values (e.g. lower than or greater than amount X) are possible.

A *Fork* splits the process flow into at least two branches which are parallel executed.

A *Join* is assigned to a specific Fork in order to unite the parallel executed process paths.

An *End* marks that the process execution stops at this point. More than one End is possible.

Referring to figure 3, all sub-elements on the right side can be attacked by threats. The following example scenarios demonstrate how risks influence business process elements:

1. *Start*: risks such as a significant raise in incoming calls given a call center scenario affect start parameters of a business process. These kinds of risks will be further on references as *business risk*.
2. *Decision*: business risks may affect the probability's distribution of outgoing edges.
3. *Resource*: risks such as an aggressive worm or an earthquake may disrupt the functionality of resources. This leads in the worst case to the interruption of the continuous execution of a business process activity. These kinds of risks are further on referenced as *resource risks*.
4. *Activity*: risks such as accidental human erratic behavior may threaten the continuous or correct execution of an activity.
5. *Resource Requirement*: Business risks such as peak periods or incorrectly planned resource needs may affect this element's characteristic.

The comprehensive information of business process elements under consideration of all risk-related elements enables the determination (e.g. via simulation) of the processes' performance.

All Business Process sub-elements can be integrated in the left-sided Business View (figure 3). However as mentioned above, only the Business Process sub-elements Start, Activity, Decision, Resource and Resource Requirement can be attacked by threats (right-sided Risk View). Figure 4 shows as demonstrative example the integration of the sub-elements Activity, Resource and Resource Requirement as well as the interconnection between the Business and Risk View.

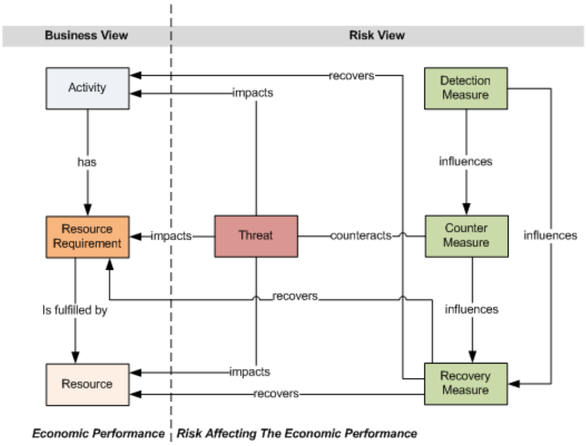

Figure 4. Reference Model applied on the Business Process Elements Activity, Resource Requirement and Resource.

We are strongly convinced that the application of our reference model facilitates the risk-aware business process modeling and simulation leading amongst others to the following benefits: (1) Simulation based determination of threats' impacts on the continuous execution of business process activities. (2) Extended business process simulation leading to results that reflect both, an economic perspective as well as a security viewpoint at the same time. (3) Modeling and simulation of manifold scenarios to enable an evaluation of different security/contingency solutions. (4) Resource utilization strategies considering risks.

5. Conclusion

In this paper, we introduce our reference model enabling risk-aware business process management. The aim and major benefit of our model is the integrated consideration of economic and risk aspects when analyzing and reengineering a company's business processes. There exist several approaches addressing the inclusion of security aspects into business process reengineering. However, we could not find an approach that comprehensively supports our modeling and simulation capabilities [9].

We want to stress that our reference model is independent from any specific modeling notation as long as the introduced elements can be covered.

For evaluation purposes, our next step is to apply our reference model within the real-world environment of an industrial partner operating in the financial sector.

6. References

[1] 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

[2] 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

[3] F. Braber, I. Hogganvik, M.S. Lund, K. Stolen, F. Vraalsen, Model-based security analysis in seven steps – a guided tour to the CORAS method, BT Technology Journal, Vol. 25 No 1, 2007

[4] British Standard Institute (BSI), British Standard – BS25999-1:2006: Business Continuity Management – Part 1: Code of practice, available at http://www.bsigroup.com, accessed Apr. 2009

[5] British Standard Institute (BSI), British Standard – BS25999-2:2007: Business Continuity Management – Part 2: Specification, available at http://www.bsigroup.com, accessed Apr. 2009

[6] S. Jakoubi, S. Tjoa, and G. Quirchmayr, ROPE: A Methodology for Enabling the Risk-Aware Modelling and Simulation of Business Processes, in ECIS, 15th European Conference on Information Systems, 2007.

[7] G. Goluch, A. Ekelhart, S. Fenz, S. Jakoubi, S. Tjoa, T. Mück, Integration of an ontological information security concept in risk aware business process management, in 41st Hawaii International Conference on System Sciences, HICSS2008, Waikoloa, HI, USA: IEEE, 2008

[8] S. Tjoa, S. Jakoubi, G. Goluch, G. Quirchmayr, , Extension of a Methodology for Risk-Aware Business Process Modeling and Simulation Enabling Process-Oriented Incident Handling Support, in proceedings of the Advanced Information Networking and Applications (AINA), 2008

[9] 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.

[10] 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.

[11] S. Jakoubi, S. Tjoa, G. Goluch, A Survey of Scientific Approaches Considering the Integration of Security and Risk Aspects into Business Process Management, *Currently under submission* at the International Workshop on Business Processes Security (BPS'09) at the 20th edition of DEXA, IEEE, 2009

[12] ISO, the International Organization for Standardization / IEC, the International Electrotechnical Commission, ISO/IEC 13335-1:2004, Information technology – Security

techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management, available at http://www.iso.org/, accessed Apr. 2009

[13] National Institute of Standards and Technology (NIST), NIST Special Publication 800-30, Risk Management Guide fir Information Technology Systems, 2002

[14] ISO, the International Organization for Standardization / PAS, Publicly Available Specification, ISO/PAS 22399:2007: Societal security — Guideline for incident preparedness and operational continuity management, available at http://www.iso.org/, accessed Apr. 2009

[15] The Business Continuity Institute (BCI), Good Practice Guidelines (GPG 2008-2), available at http://www.thebci.org/gpg.htm, accessed Apr. 2009

[16] 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

[17] D. Karagiannis, J. Mylopoulos, M. Schwab, Business Process-Based Regulation Compliance: The Case of the Sarbanes-Oxley Act, In Proceedings of the 15th IEEE International Requirements Engineering Conference, IEEE, 2007

[18] ISO, the International Organization for Standardization / IEC, the International Electrotechnical Commission, ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management, available at http://www.iso.org/, accessed Apr. 2009

[19] Object Management Group (OMG), Business Process Modeling Notation (BPMN), available at: http://www.bpmn.org/, accessed: May, 2009

[20] Object Management Group (OMG), Unified Modeling Language (UML), http://www.uml.org/, accessed: May, 2009

[21] A. W. Scheer, G. Keller, M. Nüttgens, Semantische Prozeßmodellierung auf der Grundlage "Ereignisgesteuerter Prozeßketten (EPK), in: Scheer, A. W. (Eds.): Veröffentlichungen des Instituts für Wirtschaftsinformatik, Heft 89, Saarbrücken, 1992

[22] A. W. Scheer, M. Nüttgens, ARIS Architecture and Reference Models for Business Process Management, in proceedings: Business Process Management (BPM 2000), Springer, 2000

[23] BOC, ADONIS® standard modeling language, available at: http://www.boc-eu.com/, accessed: May, 2009

[24] D. Karagiannis, S. Junginger, R. Strobl, Introduction to Business Process Management Systems Concepts, Appeared in: Scholz-Reiter, Bernd; Stickel, Eberhard (Eds.): Business Process Modeling. Springer, 1996

[25] The Business Continuity Institute (BCI), Good Practice Guidelines (GPG 2008-2), available at http://www.thebci.org/gpg.htm, accessed Apr. 2009

[26] Project Management Institute, Inc., A Guide to the Project Management Body of Knowledge (PMBOK® Guide), 3rd edition, 2004

[27] OGC (Office of Government Commerce), PRINCE2 – Managing Successful Projects with PRINCE2, Crown, 2005

[28] One Hundred Seventh Congress of the United States of America. 2002. Sarbanes-Oxley Act., http://www.law.uc.edu/CCL/SOact/soact.pdf, accessed: May, 2009

[29] European Commission, Directives, ec.europa.eu/internal_market/auditing/directives/index_en.htm, accessed: May, 2009

[30] J. Jürjens, UMLsec: Extending UML for Secure Systems Development, UML 2002, Dresden, Sept. 30 - Oct. 4, Springer, 2002

[31] A. Avizienis, J.-C. Laprie, B. Randell, and C. E. Landwehr, “Basic Concepts and Taxonomy of Dependable and Secure Computing,” IEEE Trans. Dependable Sec. Comput., vol. 1, no. 1, pp. 11–33, 2004.

7. Acknowledgement

This work was performed at the Research Center Secure Business Austria funded by the Federal Ministry of Economy, Family and Youth of the Republic of Austria (BMWFJ) and the federal province of Vienna.