A Roadmap to Risk-Aware Business Process Management

Stefan Jakoubi, Thomas Neubauer
Secure Business Austria
Vienna, Austria
{sjakoubi, tneubauer}@sba-research.org

Simon Tjoa
St. Pölten University of Applied Sciences
St. Pölten, Austria
Simon.Tjoa@fhstp.ac.at

Abstract— **The continuous, effective and efficient performance of business processes is the central element for entrepreneurial success. In order to achieve the abovementioned goal various disciplines are involved: The improvement from an economical viewpoint is mainly performed by the domain of business process management, whereas the consideration of risks and continuous execution of business processes is considered separately by risk management and business continuity management. We observed that this separation often leads to inefficiencies as decisions can be contradictory and a consistent information basis is missing. Therefore, we introduce our vision of risk-aware business process management that is capable of providing information for economic as well as for security disciplines.**

Keywords-Risk Management, Business Process Management

I. Introduction

The requirements for business processes in today's global environment are manifold. From an economical viewpoint it is essential that resources are utilized as efficient as possible and services are managed in an effective way. From a security perspective it is an objective to provide the appropriate level of availability, integrity and confidentiality. As one can see, these different aims can lead to different results although both perspectives have one overall aim: The improvement of the business process. Business process management (e.g., [1], [2]) is the predominant player when it comes to economic efficiency and effectiveness. With the rising number of security threats, it becomes inevitable to link security and economic disciplines at business process management level in order to provide companies with a business process management methodology that represents their actual business needs. Various disciplines coping with information security exist. However, for our considerations we concentrated on business continuity management (cf. [5],[6],[7],[8],[9]), risk management (cf. [3],[4]) and incident management (cf. [10]).

The major contribution of this paper is to outline future research challenges in the domain of business process security and to highlight our vision of risk aware business process management. The remainder of this paper is structured as follows: Section 2 provides an overview about current research approaches in the domain of business process security. It further identifies open research challenges of these approaches. Section 3 presents our vision of risk-aware business process management. Within Section 4 we want to conclude our work by highlighting the benefits if our vision is realized.

II. BACKGROUND

In this section we outline a selection of business process security approaches which pursuit the goal to create a tighter linkage between business process management and security. 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 [11][12]. 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 to calculate the monetary value of the process for the company. (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…" [11] 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" [11]. For expressing these relations (i.e., the searched cause-effect relations) a matrix-based description is used.

CORAS [13] 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

978-1-4244-5336-8/09/$26.00 ©2009 IEEE

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 likelihood 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. [14] present 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 [22] and COSO [23]. 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 …" [14]. (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 …" [14]. 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 [14].

AURUM: A Framework for Automated Information Security Risk Management [15], [16], [17]. As basis for their research, the authors identify the following questions which have to be addressed by organizations: (1) What are potential threats for my organization?, (2) How probable are these threats?, (3) Which vulnerabilities could be exploited by such threats?, (4) Which controls are required to most effectively mitigate these vulnerabilities?, (5) What is the potential impact of a particular threat?, (6) What is the value of security investments?, and finally (7) In which security solutions is it worth investing? The research focuses on developing concepts to meet these demands of the information security risk management (ISRM) community with the aim to support risk managers in making efficient security decisions. Figure 1 shows how the main ISRM-phases are supported. The purpose of the framework is to support investment decision makers in interactively selecting efficient security solutions. The ISRM process starts at the business process importance phase, where importance values are assigned for each required asset. Based on business process models and importance values defined by the decision maker, asset importance values are automatically calculated. In the inventory phase, the organization has to define (i) their assets, (ii) the acceptable risk level of the defined assets, (iii) the organization-wide importance of the defined assets, and (iv) the attacker profile in terms of motivation and capability. To store and interrelate this information with general information security domain knowledge the authors use a security ontology. In the threat probability phase the developed Bayesian threat probability determination extracts knowledge regarding threats, threat a priori probabilities, vulnerabilities, existing and potential control implementations, attacker profiles, and the assets of the organization from the security ontology and establishes a Bayesian network capable of calculating threat probabilities based on the aforementioned input information. In the risk determination phase relevant threat probabilities are merged with the importance information regarding the considered asset. In the control identification and evaluation phase existing and potential control implementations, their effectiveness, initial and running costs are extracted from the security ontology to support the final safeguards selection with interactive multi-criteria decision support. for the system intends to answer two fundamental ISRM questions: (i) Which IT security solutions can generally be used to mitigate the risk to an acceptable level?, and (ii) Which IT security solutions should be used to mitigate the risk cost-efficient to an acceptable level? For a more extensive survey about further approaches, we kindly refer to [18].

All mentioned approaches are substantial contributions in the field of business process security. Each of them has its own strength either in introducing interconnected layers between business, IT and risk aspects or in proposing modeling extensions in order to appropriately address security aspects when planning business processes or enhancing software development processes. However, we identified a significant gap in research efforts regarding the orientation towards business process simulations. Gartner for example stated that the "biggest benefit of business process optimization and simulation is that they deliver insight into dynamic processes so that they are designed well and operated effectively as conditions change." [21]

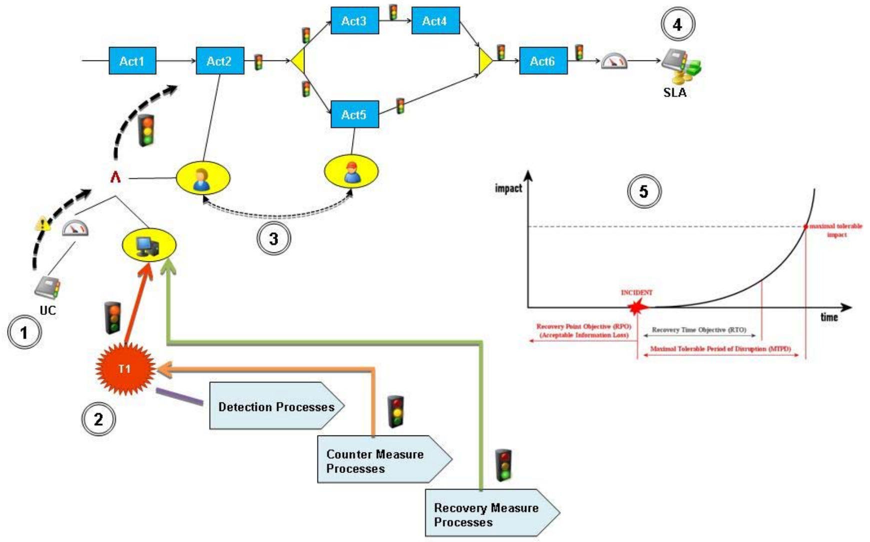
Act1
Act2
Act3
Act4
Act5
Act6
4
SLA
impact
5
maximal tolerable impact
INCIDENT
time
Recovery Point Objective (RPO) (Acceptable Information Loss)
Recovery Time Objective (RTO)
Maximal Tolerable Period of Disruption (MTPD)
3
UC
1
T1
2
Detection Processes
Counter Measure Processes
Recovery Measure Processes

Figure 1. Vision of Risk-Aware Business Process Management

III. DEFINITION OF A ROADMAP

In this section we outline our vision of risk-aware business process management. Derived from our vision we outline a roadmap addressing the main components of our idea later on in this section.

Generally, we define the term risk-aware business process management as the integration of risk aspects into business process management.

The overall objective of our research is to create a link between economic and security discipline. During our previous research we identified integration at business process level as appropriate linking point.

In order to pursuit the progress of our research we identified the following steps:

- Development of a threat model which enables the consideration of different threat categories leading to determination of impacts. This can be especially useful when performing a business impact analysis. (see Figure 2 (2))
- Development of a model, which is capable to represent detection, counter and recovery measures. We define detection measures as all measures that are capable to detect a threat. These measures determine when counter and recovery measures are invoked. The difference between counter and recovery measures within the context of this paper is as follows: Countermeasures directly counteract a threat with the goal to eliminate a threat. By contrast, recovery measures rebuild the functionality of a business process component (e.g., a resource) In order to evaluate the effectiveness and efficiency of countermeasures it is of great importance to introduce an appropriate model. (see Figure 2 (2)).
- The business process-driven security simulation provides results that express the overall impact of risks on the execution of business processes, including the determination of economic damage and time loss as well as the illustration of costs that are caused by security, countermeasures, and recovery measures. (see Figure 2 (5))
- Another issue is a methodology for the combined modelling of business processes and security resources, safeguards and threats. The use of security-enhanced business process models allows process managers to model and evaluate business processes along with security measures based on the defined security policy. In combination with reference process templates, process managers receive support in defining the optimal level of safeguards needed for mitigating threats that negatively influence the reliable execution of corporate business processes.
- Another item on our roadmap is the assessment of suppliers. This is one of the major concerns within the business continuity phase "understanding your business". Generally the impact of supplier outages is sometimes very complex to assess as oftentimes many interfaces to one supplier exist. Within our approach suppliers and their guaranteed security

requirements should be considered. An essential point within this sub-goal to evaluate whether penalties that are described in a contract are appropriate. Furthermore, it can be assessed what consequences would arise if an unplanned longer outage of a supplier takes place (see Figure 2 (1)(5)).

- Related to the previous item, we envision measuring how threat scenarios would impact the performance on service levels. This allows us to determine the whether the quality and security defined in the SLA can be met with regard to certain scenarios. This facilitates the determination which service quality is possible (see Figure 2 (4)(5)).
- The last item we consider in our vision is the dynamic allocation of resources. Dynamic resource allocation enables an organisation to better utilize their resources through the dynamic task assignment based on the skills and abilities of a resource. In our idea this should facilitate the planning of workarounds and countermeasures such as cross-skilled trainings (see Figure 2 (3)(5)).
- Finally, the aggregation and the visualization of operational data by using a business cockpit allows the proactive valuation of risk factors. This enables the early identification of potential risks and the timely definition of counter measures.

All in all, each item of the roadmap is a challenging task. Within our previous research, we already addressed the first two objectives by introducing a risk-aware business process management approach [19],[20] which is capable of modeling threats and countermeasures. We further developed a formal model to facilitate simulation ambitions. The first results of an initial prototype which was implemented using the toolset Simulink were successful.

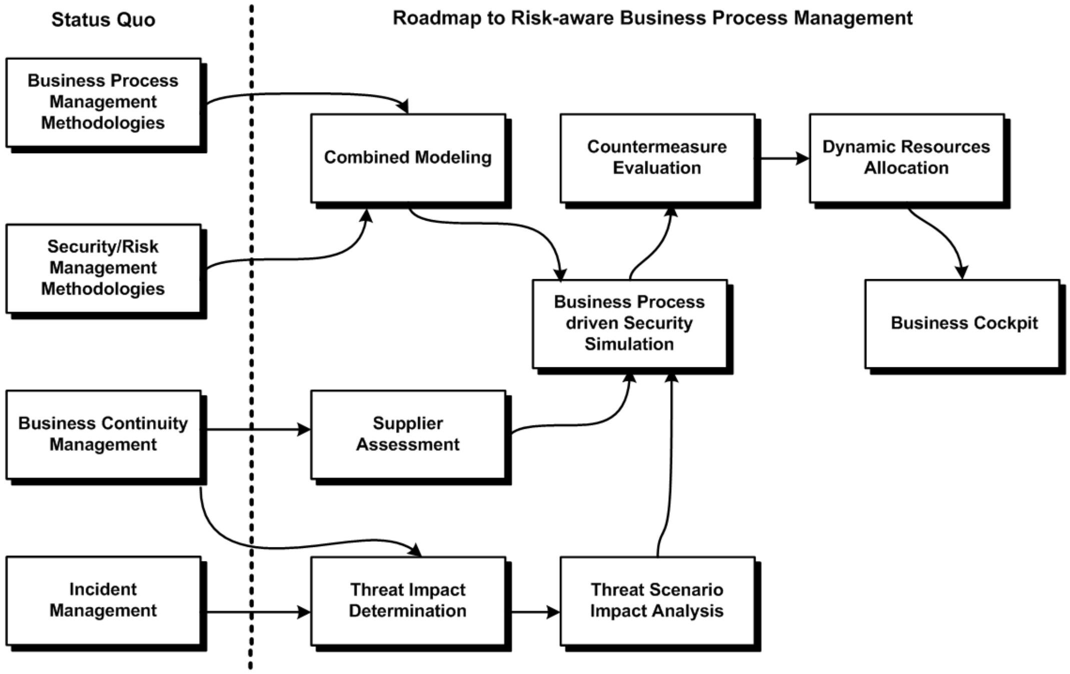
Status Quo
Roadmap to Risk-aware Business Process Management
Business Process Management Methodologies
Security/Risk Management Methodologies
Business Continuity Management
Incident Management
Combined Modeling
Countermeasure Evaluation
Dynamic Resources Allocation
Business Process driven Security Simulation
Business Cockpit
Supplier Assessment
Threat Impact Determination
Threat Scenario Impact Analysis

Figure 2. Roadmap for Risk-Aware Business Process Management

IV. Conclusion

The uninterrupted, efficient and effective of business processes is one of the central components to run successful businesses. While many international standards and best practices (e.g., Cobit) demand a tight integration between business and security objectives, the domain of business process security is still in its beginning. With this roadmap we wanted to provide an outlook of our research ambitions in order to satisfy the need for novel approaches aiming at an integration of security and economic aspects. We are still at the initial state of our research but already contributed essential results. One of the first results comprises the modeling and simulation of threats, detection-, counter-, and recovery measures. This enabled us to perform first test which should provide information about the feasibility and applicability of such an approach. The first results were very promising. However, the other research challenges are still to be solved. Summarizing we think that the importance of this research field is increasing as the challenge as IT governance ambitions are demanding a tighter integration between the various disciplines.

Acknowledgment

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 and the City of Vienna.

References

[1] D. Karagiannis, S. Junginger, and R. Strobl, Business Process Modelling. Springer, Berlin, 1996, ch. Introduction to Business Process Management Systems Concepts, pp. 81–106.

[2] W. Scheer and M. Nüttgens, "Aris architecture and reference models for business process management," in proceedings of BPM, 2000.

[3] ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management, ISO/IEC Std., 2008.

[4] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology (NIST) Std., 2002.

[5] British Standard BS25999-1:2006: Business Continuity Management - Part 1: Code of practice, British Standard Institute (BSI) Std., 2006.

[6] British Standard BS25999-2:2007: Business Continuity Management - Part 2: Specification, British Standard Institute (BSI) Std., 2007.

[7] Business Continuity Institute, "Good Practice Guidelines," 2008. [Online]. Available: http://www.thebci.org/gpgdownloadpage.htm

[8] ISO/IEC 24762:2008 Information technology - Security techniques - Guidelines for information and communications technology disaster recovery services, ISO/IEC Std., 2008.

[9] National Institute of Standards and Technology, "NIST SP800-34: Contingency planning guide for information technology systems," 2002.

[10] NIST SP800-61: Computer security incident handling guide, National Institute of Standards and Technology Std., 2004.

[11] 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

[12] 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

[13] 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

[14] 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

[15] Ekelhart, A., Fenz, S. and Neubauer, T. "AURUM: A Framework for Supporting Information Security Risk Management", 'Proceedings of the 42nd Hawaii International Conference on System Sciences, HICSS2009', IEEE Computer Society, Los Alamitos, CA, USA, 978-0-7695-3450-3, 2009, pp. 1-10.

[16] Fenz, S., Ekelhart, A. and Neubauer, T. "Business Process-based Resource Importance Determination", 'Proceedings of the 7th International Conference on Business Process Management (BPM'2009)', Springer, accepted for publication, 2009, pp. 113-127.

[17] Ekelhart, A., Fenz, S. and Neubauer, T. "Ontology-based Decision Support for Information Security Risk Management", 'International Conference on Systems, 2009. ICONS 2009. IEEE Computer Society, 2009, pp. 80-85.

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

[19] S. Jakoubi, S. Tjoa, and G. Quirchmayr, "Rope: A methodology for enabling the risk-aware modelling and simulation of business processes," in Fifteenth European Conference on Information Systems, 2007, pp. 1596–1607

[20] S. Jakoubi, G. Goluch, S. Tjoa, and G. Quirchmayr, "Deriving resource requirements applying risk-aware business process modeling and simulation," in 16th European Conference on Information Systems, 2008, pp. 1542–1554.

[21] Gartner Inc.: Misconceptions on Process Optimization and Simulation. http://blogs.gartner.com/jim_sinur/2009/01/27/misconceptions-on-process-optimization-and-simulation/ (2009)

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

[23] Committee of Sponsoring Organizations of the Treadway Commission. 2004. Enterprise Risk Management: Executive Summary. http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf