Chapter 6
Risk-Aware Business Process Management—Establishing the Link Between Business and Security

Stefan Jakoubi, Simon Tjoa, Sigrun Goluch, and Gerhard Kitzler

Summary Companies face the challenge to effectively and efficiently perform their business processes and to guarantee their continuous operation. To meet the economic requirements, companies predominantly apply business process management concepts. The substantial consideration of robustness and continuity of operations is performed in other domains such as risk or business continuity management. Applying these domains separately, analysis results may significantly differ as valuations from an economic and risk point of view may lead to deviating improvement recommendations. Observing developments in the past years, one can see that regulative bodies, the industry, and the research community laid a special focus on the tighter integration of business process and risk management. Consequently, the integrated consideration of economic, risk, and security aspects when analyzing and designing business processes delivers enormous value to achieve these requirements.

In this chapter, we present an survey about selected scientific approaches tackling the challenge of integrating economic and risk aspects. Furthermore, we present a methodology enabling the risk-aware modeling and simulation of business processes.

S. Jakoubi (✉) · S. Goluch · G. Kitzler
Secure Business Austria, 1040 Vienna, Austria
e-mail: sjakoubi@sba-research.org

S. Goluch
e-mail: sgoluch@sba-research.org

G. Kitzler
e-mail: gkitzler@sba-research.org

S. Tjoa
St. Poelten University of Applied Sciences, 3100 St. Poelten, Austria
e-mail: simon.tjoa@fhstp.ac.at

F. Xhafa et al. (eds.), *Complex Intelligent Systems and Their Applications,*
Springer Optimization and Its Applications 41,
DOI 10.1007/978-1-4419-1636-5_6, © Springer Science+Business Media, LLC 2010

6.1 Introduction

Maximizing revenues has always been and will always be the outmost objective of profit oriented companies. Business process management assured within the last years its position as predominant player in modeling and simulating a company's business processes providing significant decision support in optimizing workflows and resource utilizations. Thus, it is no surprise that Gartner outlines in its CIO report 2009 (Gartner Inc. 2009) that the improvement of business processes is number one priority. Let us take a closer look at the statement "improvement of business processes." It is obvious that for profit maximizing ambitions, the economic effectiveness and efficiency of business processes has to be optimized. The reduction of execution and waiting times, more efficient process activity structures, and resource allocations are only a few examples how to improve the executed business processes from an economic point of view. At the same time, one must not forget to in-depth consider requirements from business on its processes such as confidentiality, integrity, and availability in order to mention the most popular security goals. The best possible optimized business process is worthless if it cannot be executed, for example, in the case of a complete data center outage. Serious legal implications would arise if highly sensible health data is disclosed to unauthorized entities. A company can hardly be satisfied if, for instance, the car manufacturing process is accelerated for ten percent but a resulting recall initiative annihilates this improvement and furthermore requires significant additional budget for taking reputation rehabilitation actions. There exist diverse classifications of these threats (National Institute of Standards and Technology 2002; BSI 2004; International Organization for Standardization 2004) ranging from accidents (e.g., unavailability of ICT resources or the absence of strategic personnel) to natural catastrophes (e.g., earthquakes) and to deliberate acts (e.g., sabotage or theft). Risk management has been the major player addressing these issues. In the past years it got significant support through the evolvement and acceptance of further domains such as incident, disaster recovery, and business continuity management (National Institute of Standards and Technology 2004; British Standard Institute 2006, 2007; International Organization for Standardization 2008). The European Network and Information Security Agency (ENISA) states that "it is very difficult to isolate all the disciplines related to planning for and recovering from an incident which threatens an organization either from an internal or external source. All the disciplines are closely related and there are areas of cross-over…" (European Network and Information Security Agency 2008). However, diverse associations and regulative bodies emphasized the importance of seriously tackling risks while improving business performance which became manifest in exemplarily the Sarbanes Oxley Act (One Hundred Seventh Congress of the United States of America 2002) or the 8th audit directive of the European Union (European Commission 2010). Searching in relevant libraries, one can furthermore observe that over the last years also the scientific community increased its research efforts in trying to integrate risk and economic business aspects. As mentioned above, business process modeling and simulation is the adequate technique to support the economic analysis of a company's business processes. Simultaneously, there are several research results regarding the integration of risk aspects and security requirements into business process analyses. However, these approaches do not focus on modeling characteristics that are required for performing (risk-aware) business process simulations. As a consequence, business process simulations support economic analyses and optimizations but neglect the consideration of security and business continuity requirements.

The major objective of this book chapter is to address these shortcomings. Therefore, we, on the one hand, provide selected related research and, on the other hand, present our approach for risk-aware business process management. The term risk-aware business process management is understood as the integration of a risk perspective into business process management. The rest of this chapter is organized as follows. Section 6.2 gives an overview about selected related research. Section 6.3 provides information about required steps to perform risk-aware business process management. In Sect. 6.4, we introduce our proposed reference model. In Sect. 6.5, we outline the business case for applying our approach and give examples for application scenarios. We conclude this chapter in Sect. 6.6 and give an outlook on future research challenges.

6.2 Related Work

In this section, we give a brief overview about selected research results aiming at the incorporation of risk aspects into business process modeling and analyses. For detailed information on the included approaches, we kindly refer to the according references of the provided related work.

Sackmann extends current risk management methods with a business process-oriented view leading to an IT risk reference model (Fig. 6.1), which builds the bridge between the economic and more technical layers including vulnerabilities (Sackmann 2008; Sackmann et al. 2009). 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…" (Sackmann 2008) 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" (Sackmann 2008). For expressing these relations (i.e., the searched cause-effect relations), a matrix-based description is used.

CORAS (Braber et al. 2007) 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

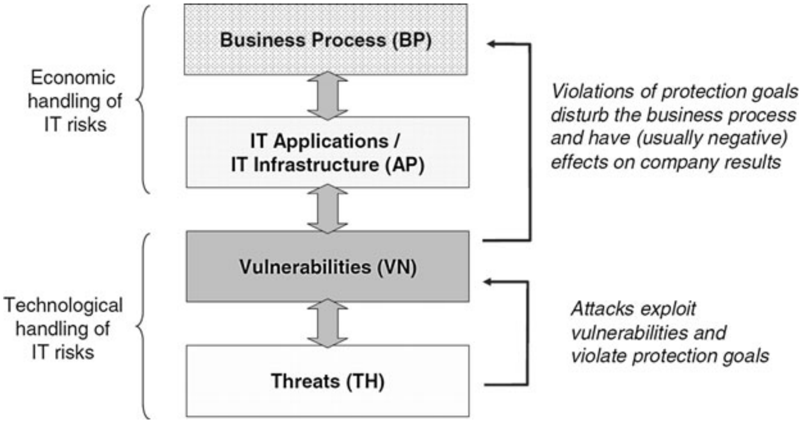

Economic handling of IT risks
Business Process (BP)
IT Applications / IT Infrastructure (AP)
Violations of protection goals disturb the business process and have (usually negative) effects on company results
Technological handling of IT risks
Vulnerabilities (VN)
Threats (TH)
Attacks exploit vulnerabilities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

Fig. 6.1 IT risk reference model (Sackmann 2008)

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. (2007) 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. The six-step 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…" (Karagiannis et al. 2007). (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…" (Karagiannis et al. 2007). 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 Karagiannis et al. (2007).

AURUM is a framework for automated information security risk management (Ekelhart et al. 2009a, 2009b; Fenz et al. 2009). 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. The detailed specification of the developed concepts introduces new automated risk management approaches on a conceptual level and poses as template for tool implementations. Figure 6.2 shows how the main ISRM-phases are supported. The purpose of the entire 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 an overall importance value for each, asset importance values are automatically calculated. In the inventory phase, the organizations 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

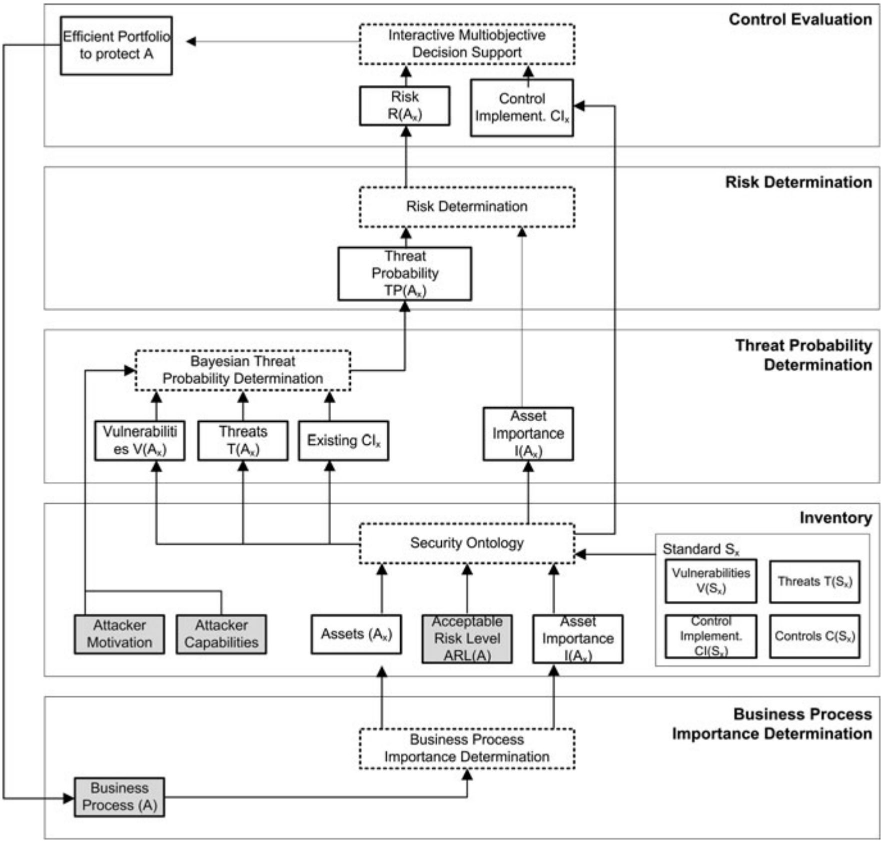

Control Evaluation
Efficient Portfolio to protect A
Interactive Multiobjective Decision Support
Risk R(A$_x$)
Control Implement. CI$_x$
Risk Determination
Risk Determination
Threat Probability TP(A$_x$)
Threat Probability Determination
Bayesian Threat Probability Determination
Vulnerabilities V(A$_x$)
Threats T(A$_x$)
Existing CI$_x$
Asset Importance I(A$_x$)
Inventory
Security Ontology
Standard S$_x$
Vulnerabilities V(S$_x$)
Threats T(S$_x$)
Control Implement. CI(S$_x$)
Controls C(S$_x$)
Attacker Motivation
Attacker Capabilities
Assets (A$_x$)
Acceptable Risk Level ARL(A)
Asset Importance I(A$_x$)
Business Process Importance Determination
Business Process Importance Determination
Business Process (A)

Fig. 6.2 The AURUM process

costs are extracted from the security ontology to support the developed interactive multicriteria decision support. Information regarding the relevance of existing and potential control implementations is extracted from the Bayesian threat probability model. Using the extracted data as input for the developed multicriteria decision support methodology, a solution concept is provided for 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?

Modeling security requirements in business processes is also the goal of an extension of UML 2.0 by Rodríguez et al. (2006). According to the authors, this is essential since software developers derive necessary requirements for software design and implementation from business processes (Rodríguez et al. 2006). 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. The proposed extension makes use of activity diagrams to allow the definition of business processes security requirements (Fig. 6.3).

Zur Muehlen and Rosemann identify risk as an inherent property of every business process (zur Muehlen and Rosemann 2005). Therefore they propose to counteract the trend of considering risk only from a project management viewpoint and to tackle the topic of risk management in the context of business process management. They consequently introduce a taxonomy (Fig. 6.4) including process-related risks and their appliances concerning the analysis and documentation of business processes. Additionally, they propose a taxonomy for business processes 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 risks. To capture risks in the context of business processes, the authors introduce four interrelated model types:

1. The Risk Structure Model provides information regarding the relationship between risks.
2. The Risk Goal Model represents a risks/goals matrix.
3. The Risk State Model captures the dynamic aspects of risks and consists of the different object types: risk, consequence, and connectors.
4. Event-driven Process Chains (EPCs) are extended to consider risks, enabling the assignment of risks to individual steps in the specific process.

The need for a holistic business view on risk management is addressed by Neiger et al. (2006). Accordingly, value-focused process engineering, which creates links between business processes and business objectives at the operational and strategic levels, is utilized. This value-focused process engineering approach is applied to risk management models, resulting in a risk-oriented process management view. The overall model consists of four steps:

1. To identify relevant process risks, business objectives are decomposed, while each process activity is examined in order to identify further relevant risks.
2. To identify risks and to determine related processes, value-focused approaches are used.
3. To identify the best process structure to meet the business objectives, process configurations are suggested.
4. To enable the selection of an optimal process configuration, alternative configurations and their corresponding results that meet the identified risk minimization objectives are finally compared.

Focusing on business process availability, Milanovic et al. (2008) present a framework for modeling availability considering services, underlying ICT infrastructure and human resources. To model these relations, the authors adapt a service-enabled architecture (Fig. 6.5). Moreover, a fault-model with two failure modes (Temporal/Value) is used, thus enabling an analytical assessment procedure:

1. Define the business process following a process modeling language.
2. Refine activities by modeling atomic services.

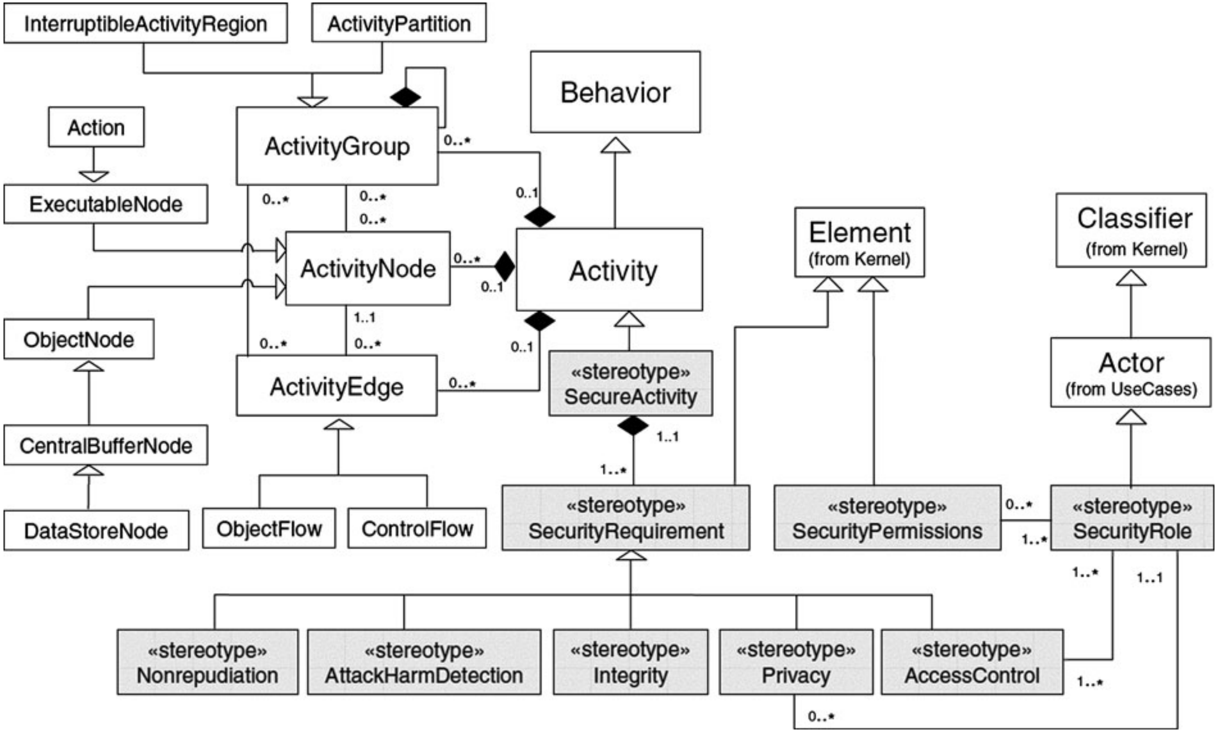


Fig. 6.3 Extending the UML 2.0 metamodel with security stereotypes (Rodríguez et al. 2006)

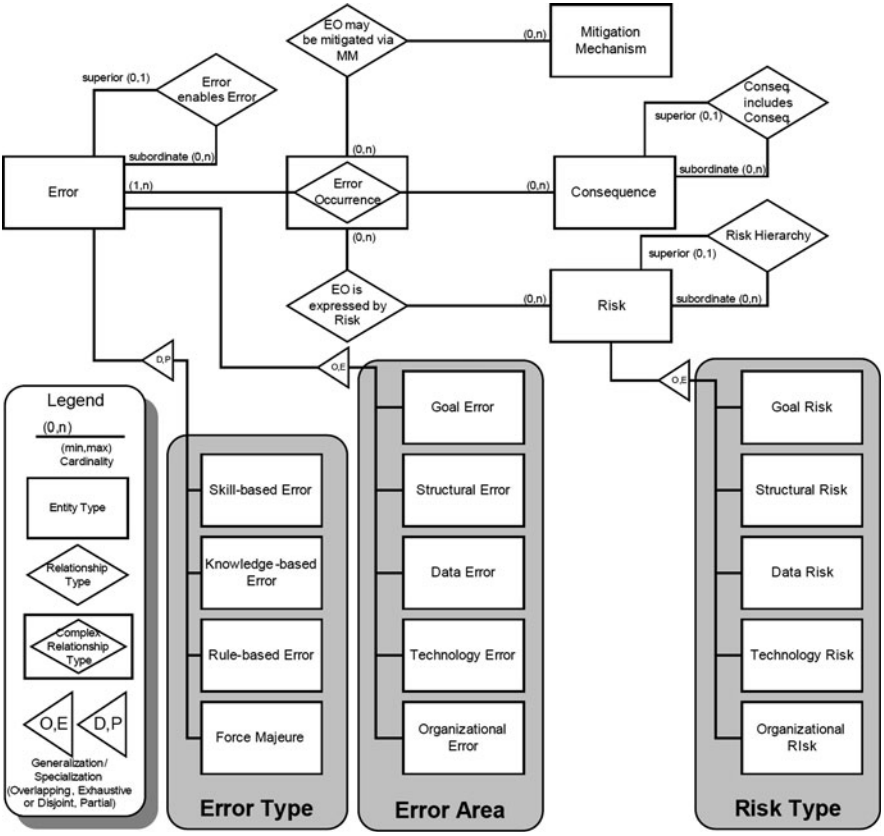
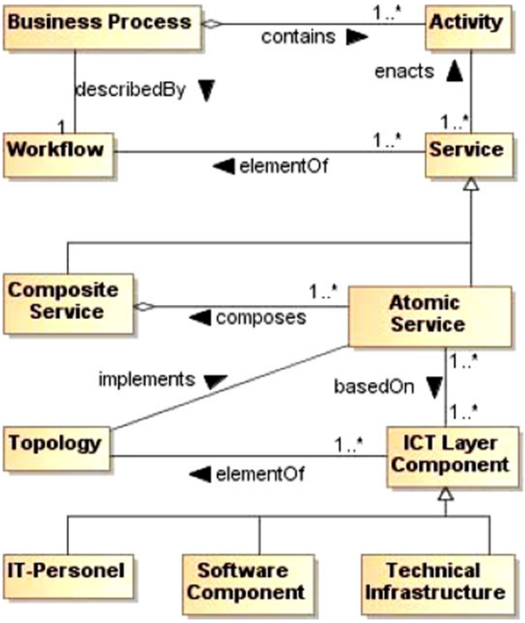


Fig. 6.4 Risk taxonomy (zur Muehlen and Rosemann 2005)

3. Create an infrastructure graph.
4. Map services to infrastructure components. Transform paths for service executions into Boolean expressions.
5. Map business processes to atomic services. The functional dependency between business process, service and ICT-layer availability is the result.
6. Transform the Boolean expressions into reliability block diagrams/fault trees to calculate steady-state availability.
7. Calculate the availability of business process and services by solving/simulating the model generated within the abovementioned steps.

Regarding the compliance of business processes, Weber et al. (2008) propose an approach to validate whether the states reached by a process are compliant with a set of constraints or not. This enables compliance checking of a new or altered process against a given constraints base and of the process repository against a different or changed constraints base (Fig. 6.6). The authors formalize and utilize a class of compliance rules and annotated process models respectively.

Fig. 6.5 Service-enabled architecture (Milanovic et al. 2008)



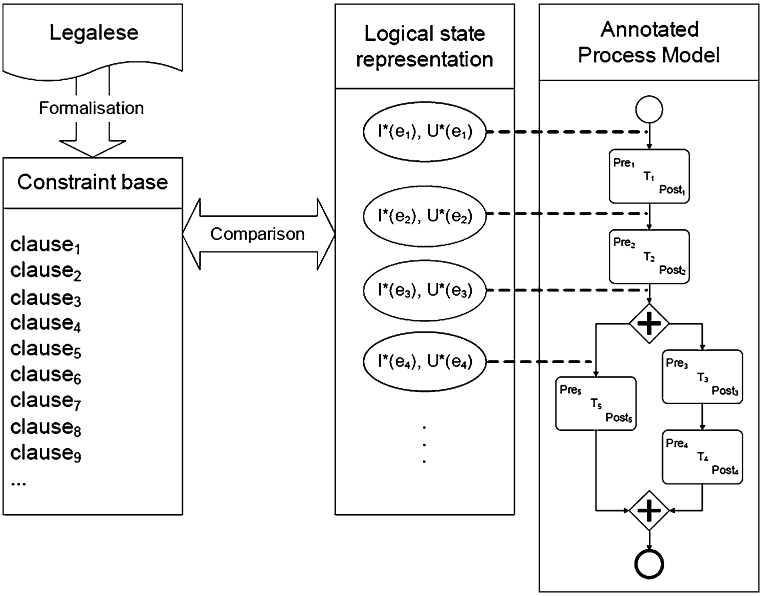


Fig. 6.6 An overview of the framework (Weber et al. 2008)

Sadiq et al. (2007) also address the problem field of business process compliance and identify the need for systematic approaches to understand the interconnection

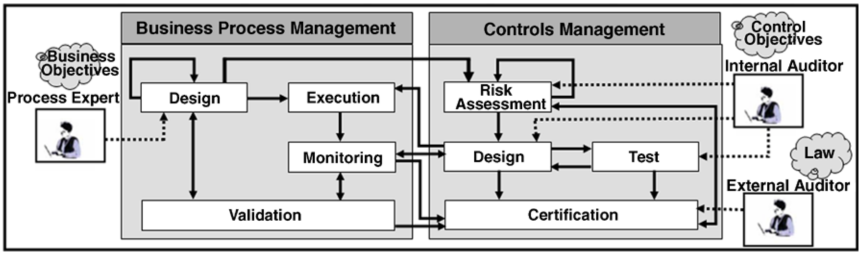


Fig. 6.7 Interconnect of process management and controls management (Sadiq et al. 2007)

and dependency between business and control objectives. Accordingly, the authors introduce a modal logic based on normative systems theory, dealing with the effective modeling of control objectives and their propagation onto business process models (Fig. 6.7).

Jallow et al. (2007) propose a framework for risk analysis in business processes with focus on cost, time and performance/quality analyses. The framework consists of the following six steps (Fig. 6.8):

1. Model the activities of the business process.
2. Determine for each activity the considered dimensions (i.e., cost, time, and output). As within a specific risk analysis only one dimension can be evaluated, the objective of each analysis has to be defined.
3. Identify risk factors, probability of occurrence, and impact.
4. Assumptions regarding the risk impact should be defined in order to consider uncertainties associated with risks. The authors use a three-point estimate expressed as triangular distribution.
5. Calculate each identified risk by multiplying the occurrence probability with the impact. “The impact is not a discrete value but a serious of values generated by the simulation based on the distribution.”
6. Calculate forecasts for each activity and accumulative for the whole process.

   A prototypical framework implementation has been performed using Microsoft Excel using the add-on software Crystal Ball™.

Above, we gave a representative overview of several research approaches that aim to establish an integrated view on security, risk and business process management. It is not meant to be a holistic domain overview, but we think the selection gives the reader a good overview about developments in the recent years. Summarized, existing approaches achieved the following research results:

1. Rule-based validation of process security and selection of counter measures.
2. Extension or customizations of modeling languages (e.g., UML 2.0) by introducing security requirements modeling capabilities.
3. Stronger linkage of risk and business process management (e.g., via a taxonomy or via a reference model linking threats, vulnerabilities, ICT resources, and business processes).
4. Calculation of business process availability.

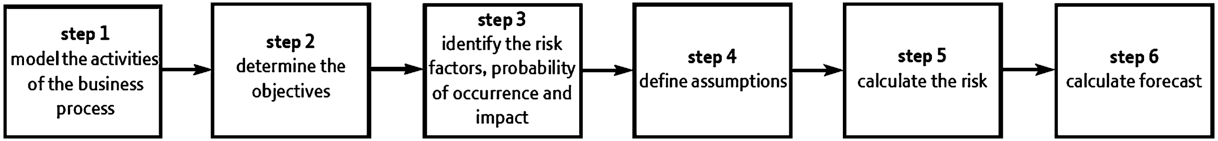


Fig. 6.8 The risk-based proposed framework (Jallow et al. 2007)

5. Integration of business and compliance objectives.
6. Determination of risk impacts on the business process activity layer using Monte Carlo simulation.

The mentioned approaches contributed substantial research in the field of business process security. However, we still miss a concept meeting the following objectives.

1. Integrated modeling concept:
   a. Business process activities
   b. Required resources
   c. Threats endangering these resources
   d. Detection, counter, and recovery measures
   e. Relations between these components
2. Concept for the simulation-based determination of risk impacts (e.g., time, costs, backlogs, etc.) on resources and/or directly business process activities considering the interaction between threats and detection-, counter-, and recovery measures.

6.3 Steps Required to Perform Risk-Aware Business Process Management

In this section we introduce the necessary steps to perform risk-aware business process management. The proposed steps must not be understood as rigid or inflexible but as requirements guidelines when setting up a respective program. The steps are derived from best-practices-guides and standards of the business process management risk management and business continuity domains. Figure 6.9 outlines the proposed steps.

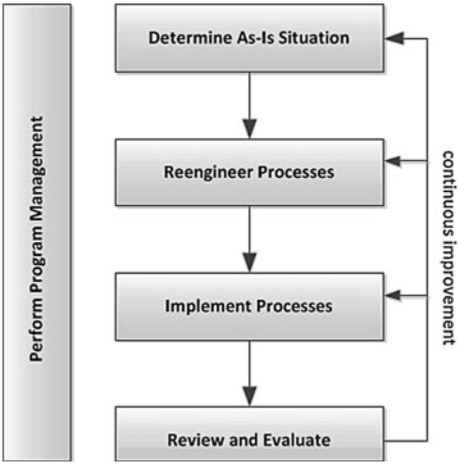


Fig. 6.9 Recommended phases for performing risk-aware business process management (Jakoubi and Tjoa 2009)

6.3.1 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:

- Scope: The Scope of the program is essential to guarantee that the program achieves the desired results. It should be clearly defined and documented which areas of an organization should be addressed by the program. Typical content of the scope definition is the identification of included business units and core processes, the geographic scale, and time and budget constraints. A good program scope definition can reduce costs. However, one should be aware that a too tight program scope definition could lead to deficiencies in the quality of results as important dependencies could be overlooked. To ensure the correctness and appropriateness of the scope, senior management should sign-off the scope of the program.
- Organizational Environment: The analysis of the Organizational Environment provides information of the vision, business objectives, and strategies of a company, as well as the market in which the company currently operates or wants to operate (e.g., competitors, customers). A clear understanding of the business forms the foundation for the evaluation of risks and the determination of mitigation strategies. The following example should clarify the statement: A company having a monopole obviously has other mitigation requirements than a company facing strong competition.
- Evaluation Criteria: In order to ensure that the program is achieving the expected goals, it is essential to introduce Evaluation Criteria. When defining these criteria, one should consider that they must be measurable in order to be evaluated. 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: In order to set up an effective program, Roles and Responsibilities for the program planning, execution, and controlling have to be defined. Another critical success factor for the program is senior management buy-in. It is always a good idea to have a supporting program sponsor within the board.
- Program Steering: 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.

6.3.2 Determine As-Is Situation

The objective of this step is to gather information for further analysis steps. In order to ensure appropriate information, we recommend the following steps:

- Core Process Identification: In order to conduct risk-aware business process management, it is required to acquire the core processes of an organization. All business units should be surveyed to ensure sufficient information about core activities, possible execution paths, and their probabilities is gathered. The business processes should be mapped to the organization's goals. Furthermore, process (activity) characteristics such as execution times and costs, and the value of the process (e.g., monetary value, intermediate products) have to be determined. Additionally, interdependencies to internal and external units should be recorded.

- Resource Identification: In this step required resources, their interdependencies, and their assignment to activities are determined. Also dependability requirements should be acquired in the resource identification phase.
- Risk Identification: The objective of this phase is to get a clear understanding about the risks a company faces. At least two types of risks should be considered when performing the risk identification: (a) Business Risks affecting process characteristics (e.g., change of invocation frequency, input parameters, change of decision probabilities). Business risks can be determined by historical data such as nonpayment of credits per year or similar key figures. (b) Resource Risks affecting dependability attributes such as confidentiality, integrity, and availability (e.g., worm disrupting the functionality of servers). The analysis of the as-is situation regarding resource related threats can be supported by tools used within the organization such as data leakage prevention solutions or event correlation tools. Furthermore, risks can be identified by using external information such as the determination of environmental vulnerability to natural disaster from meteorological institutes or information security trends from research organizations.
- Detection, Counter, and Recovery Measure Identification: The Detection, Counter, and Recovery Measure Identification deliver information about implemented measures and processes. Detection measures (e.g., fire detectors) are the basis for a successful response. Effective detection mechanisms reduce the time period until implemented counter and recovery measures may be invoked. Internal and external detection mechanisms are considered within our model. However, depending on the detection method, the initiated counter and recovery measures may vary. Counter measures can either be preventive or reactive in nature. Preventive counter measures (e.g., nonsmoking policy) reduce the occurrence probability, while reactive counter measures (e.g., fire sprinkler) decrease the potential impact by fighting the threat. Recovery measures (e.g., restore of back-up tapes) within our approach reestablish the functionality of disrupted resources.

The acquired information is modeled according to the proposed reference model, which is described later in this work, to enable further analyses such as risk-aware business process simulations as introduced in (Jakoubi et al. 2007, 2008; Goluch et al. 2008; Tjoa et al. 2008a, 2008b).

6.3.3 Reengineer Processes

The Reengineer Processes phase aims at improving the processes from an economic and from a security point of view. However, the main driver of this step is definitely the business. Through our novel risk-aware business process simulations the risk perspective is strongly integrated in the process improvement process. The following phases have at least to be performed:

1. Business Impact Analysis: The Business Impact Analysis examines the impacts (e.g., financial, reputational) of resources' and/or activities' disruptions over time. The outputs of a business impact analysis are key figures such as the Maximum Tolerable Period of Disruption (MTPD) or the Recovery Point Objective (RPO) (Business Continuity Institute 2008).
2. Risk Analysis: The Risk Analysis identifies risks and their impact on dependability attributes of resources and/or activities. The step concludes by determining how risk should be addressed (according to the company's risk strategy) and how the process should be prioritized.
3. Identification of Improvement Options: The result of the step Identification of Improvement Options is a set of improvement alternatives for economic and security improvements. The options are presented to the senior management which has to sign-off the options that should be implemented.
4. Redesign of Processes: Once the improvement options are selected, 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 risk-aware process simulation can be used to find a proper design for the process.
5. Evaluation: The Evaluation step 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 depending on the deficiency found. This assures the quality of the design and minimizes the threat of expensive design errors.

As described in (Jakoubi et al. 2007, 2008; Tjoa et al. 2008b), our concept of risk-aware business process modeling and simulation can be applied to support these phases.

6.3.4 Implement Processes

The Implement Processes phase aims at implementing the designed processes. Steps necessary to apply new processes to an organization comprise at least the following:

1. Project Setup: 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. Furthermore the clear scope of the project has to be defined, and evaluation parameter should be determined. Additionally, typical project management activities such as project controlling have to be carried out.
2. Implementation: The next step is the Implementation of the specific projects. While the implementation step it is important to evaluate the technical solutions in order 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. If necessary, awareness trainings should be carried out.

3. Evaluation: 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.

In general, it is hardly possible to estimate the duration of the implementation phase as it significantly depends on the approved and budgeted scope of the implementation project. However, regarding projects with duration longer than one year, it would definitely be feasible to define frequent controls of intermediate deliverables (e.g., every 3 months) to facilitate adequate project steering. Milestones with assigned deliverables should be planned at least biannually, and a greater project status evaluation should be performed at least annually.

6.3.5 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.

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

6.4 A Reference Model for Risk-Aware Business Process Management

In this section, we firstly introduce our reference model enabling risk-aware business process management. Later in this chapter, we outline the set of recommended business process and risk-related elements for our approach. We decided to support this specific set in order to ensure support for a broad range of modeling notations. Figure 6.10 schematically shows our reference model. Summarizing the foundation of the reference model, which can be found in (Jakoubi et al. 2007, 2008; Goluch et al. 2008; Tjoa et al. 2008a, 2008b), the concept of risk-aware business process modeling can be described as follows: Threats put business process elements (e.g., an activity or a resource) in danger. A successful attack of a threat can lead to an interruption or a delay in the execution of the business processes. In order to protect a company and its asset, three functions are required (i.e., detection, counteracting, recovery). In the following we briefly describe how we realized the functions within our reference model. Detection measures influence the time period until when counter and recovery measures are invoked. Counter measures can reduce either the

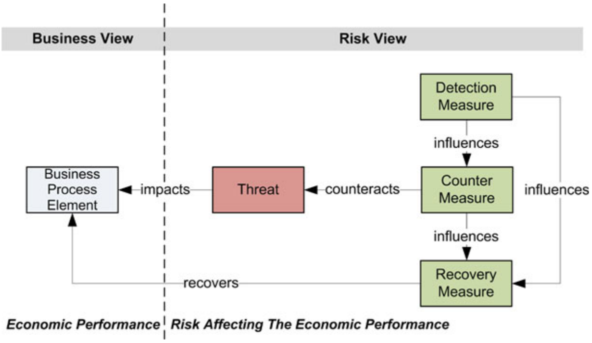


Fig. 6.10 General reference model (Jakoubi and Tjoa 2009)

likelihood of a threat's occurrence or directly counteract a threat. Recovery measures reestablish the functionality of the business process (e.g., recovery of an affected resource). Therefore our risk view contains the succeeding elements:

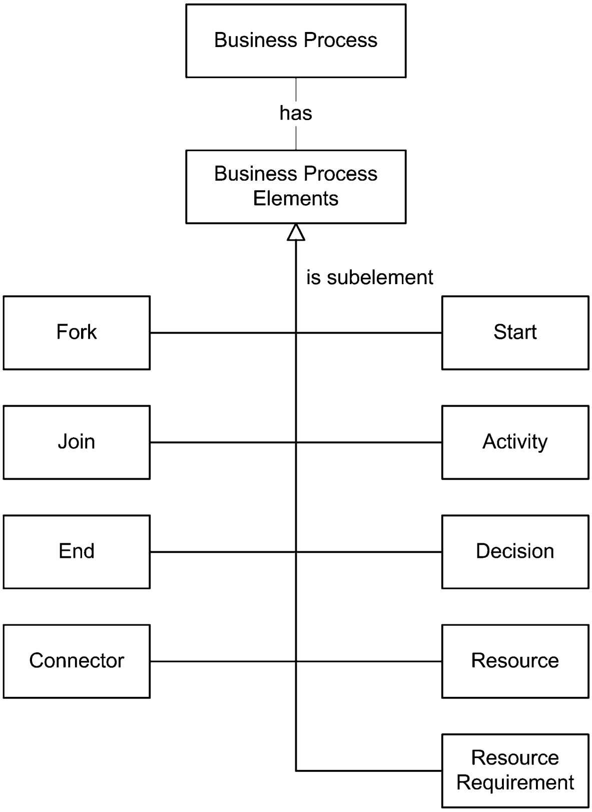
- Threats containing an occurrence probability affecting business process elements with a certain impact.
- Counter Measures either reduce the occurrence probability of a Threat (i.e., preventive) or the potential impact of an occurred Threat (i.e., reactive).
- A Recovery Measure reestablishes the functionality of impacted resources and/or activities.
- A Detection Measures influences the time periods until Counter and Recovery Measures are invoked.

Within our proposed approach each of the abovementioned elements can be represented as a process. In order to consider the behavior of threats, detection-, counter-, and recovery measures, we propose the usage of according functions. Exemplarily, an impact function represents the effect of a threat "fire" on the availability attribute of the resource "server room." The more expertise and historical data is at hand, the easier is the derivation of representative functions. Exemplarily, under the assumption of a severe earthquake and the absence of seismic safeguards, the determination of the threat's impact function will be straightforward. In contrast, the challenge of an "insider" threat's impact function will definitely be more difficult to solve. For assigning threats and resources, there are international standards and best-practices (e.g., BSI 2004) provide sufficient guidance. A possibility from the scientific perspective would be the usage of a security ontology (Goluch et al. 2008).

Generally our reference model does not require a specific process modeling language in order to address a broad audience. The quality of results however could vary. Therefore we recommend a minimal set of required business process elements which are outlined in Fig. 6.11. The elements on the right side (i.e., start, activity, decision, resource, resource requirements) could currently be affected by threats in our model. In order to clarify our needs we shortly describe the elements and their functionality in the succeeding paragraphs.

Within our approach, a Business Process is the container for all further elements. A Business Process can consist of the succeeding Business Process Elements:

Fig. 6.11 Minimal set of business process elements (Jakoubi and Tjoa 2009)



- 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. Risks that affect this element change the start parameter of the process. An example would be an increase of incoming calls within a call center. These kinds of risk will be further referred as business risk.
- An Activity transforms by definition inputs into outputs by using a specific set of resources. In order to conduct suitable analysis an activity should at least possess the economic attributes Execution Time and Costs. For risk analysis purposes, an activity should also have the following further risk-related attributes:

  1. A Completion Function which may be affected by an occurred threat. This enables us to consider delays of activities;
  2. The flag Interruptible which describes whether the execution of the activity may be delayed or the activity has to be totally reexecuted;
  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.

Risks that directly affect an activity threaten the continuous or correct execution of an activity. Examples would be accidental human erratic behavior caused by lack of knowledge.

- A Resource is required to perform 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. Risks can affect the attributes of resources such as the availability of resources. Examples of threats that could affect resources are an aggressive worm or an earthquake which may disrupt the functionality of resources. Risks affecting the resources will be further referred as term Resource Risk.
- 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. Typical risks affecting this element are business risks such as peak periods or incorrectly planned resource needs may affect this element's characteristic.
- 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. Business risks may affect the probability distribution of outgoing edges.
- 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.

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 subelements can be integrated in the left-sided Business View (Fig. 6.11). However as mentioned above, only the Business Process subelements Start, Activity, Decision, Resource, and Resource Requirement can be attacked by threats (right-sided Risk View). Figure 6.12 shows as demonstrative example the integration of the subelements Activity, Resource, and Resource Requirement and the interconnection between the Business and Risk View.

6.5 Application Scenarios

In this section we first want to outline two business cases in order to show the capabilities of our approach. Secondly, we outline further application scenarios of our approach with a special focus on resource utilization. For the sake of clarity,

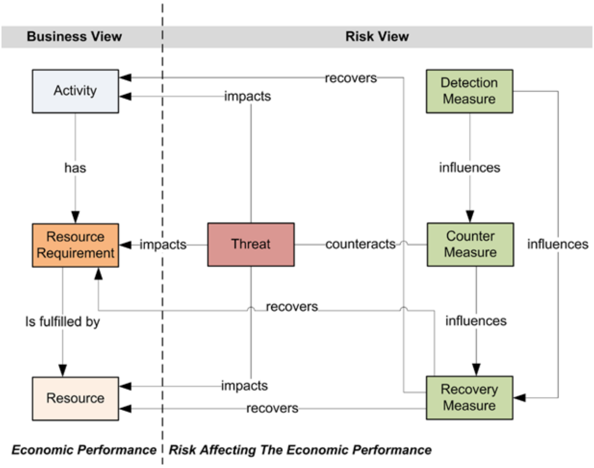


Fig. 6.12 Reference model applied on the business process elements activity, resource requirement and resource (Jakoubi and Tjoa 2009)

these are stylized use cases. Figure 6.13 gives a conceptual overview about our approach which serves as basis for two demonstrative service level analysis scenarios within the company ACME: (1) A threat (T1) endangers the assigned resource and (2) the outage of the underpinning contract (UC) shall be evaluated in the course of a what-if simulation. In scenario 1, a threat puts an assigned resource (R) in danger. In order to better demonstrate the effects of a threat our resource model indicates that R is not redundantly sized but required (i.e., logical and relation). A disruption of the resource would therefore cause a delay in the execution of the business process activity 2 (Act 2). In a nutshell, detection measures try to detect an occurred threat and invoke corresponding counter measures which try to eliminate the threat. Subsequently—or partially overlapping—recovery measured try to restore the disrupted resource. The bottom line is that in the course of the simulation, the threat is eliminated and the resource restored. Thus, Act 2 can be again executed. Through our risk-aware business process simulation, we are able to determine additional costs and times through invoking detection-, counter-, and recovery measures and to consider delays or total outages in the activity's execution. This can consequently be used to analyze signed Service Level Agreements. One example outcome is the probability that—on the basis of the modeled company's as-is situation and one or more threat scenarios—the signed agreement will be breached leading to arising penalties for ACME. In scenario 2, an underpinning contract (UC) is analyzed. There, three interesting questions for ACME are: (1) "to which availability extent the agreed service is required?", (2) "what are the impacts of a UC outage (i.e., contract breach of ACME's service provider)?", and (3) consequently, "which penalty has to be agreed to adequately transfer the financial risk?". In the modeled as-is situation, there is no continuity plan for UC implemented, thus it is according to the resource model completely required to perform Act 2. Applying our risk-aware business process simulation, ACME can simulate various contract options (e.g., bronze level with 90 percent guaranteed availability, silver level with 99 percent availability, and gold level with 99.99 percent availability). Consequently, the

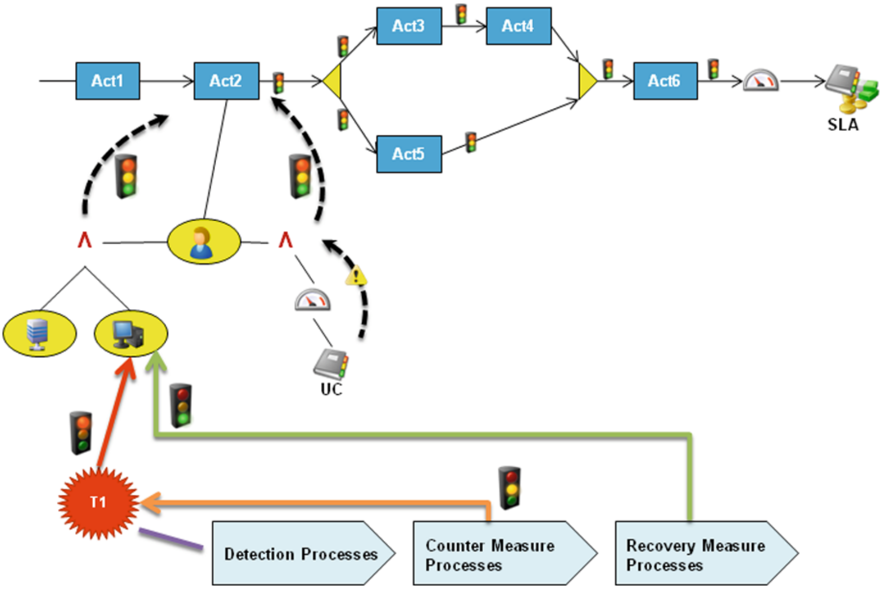


Fig. 6.13 Conceptual risk-aware service level analysis

simulated situations can be evaluated for one business year taking at least contract costs, outage probabilities, possible business process executions paths (e.g., through decision elements), peak periods (e.g., at the end of the accounting year), and resulting (financial) impacts into account.

We implemented a prototype within the Matlab® module Simulink® (The MathWorks 2010). The following figures sketch extracts from our simulation results for scenario 2. The bronze level selection would cause significant backlogs (see Fig. 6.14) and would lead to potential service level breaches for ACME under the assumption that the vertical dotted line is the evaluation baseline. In comparison to the selection of the silver level (see Fig. 6.15), the results support decision makers to choose the silver level. Further investments to buy the more comprehensive gold level are questionable as the silver level seems to be sufficient.

In the following we want to outline further application scenarios which focus on resource utilization and are described in detail in Jakoubi et al. (2008).

- Simulation-based determination of resources working capacities (in percent) in case of reallocation between processes, for example, a resource is required for 100 percent by its dependent business process and simultaneously for 40 percent by a threat impact process. Thus, its theoretically required working capacity is 140 percent.
- Simulation-based determination of the changing resource utilization during threat scenarios, for example, the reallocation of personnel from a business process in order to counteract an occurred threat affecting the operability of another (e.g., higher prioritized) business process.

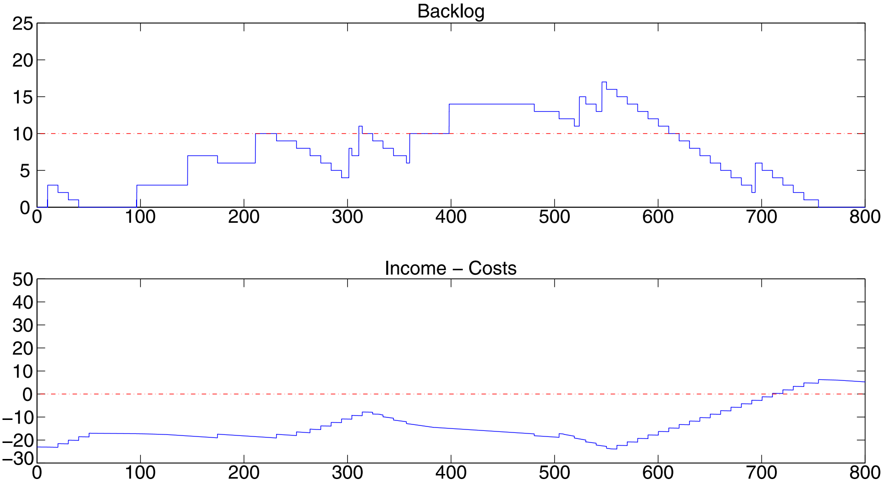


Fig. 6.14 Simulation result excerpt: bronze level

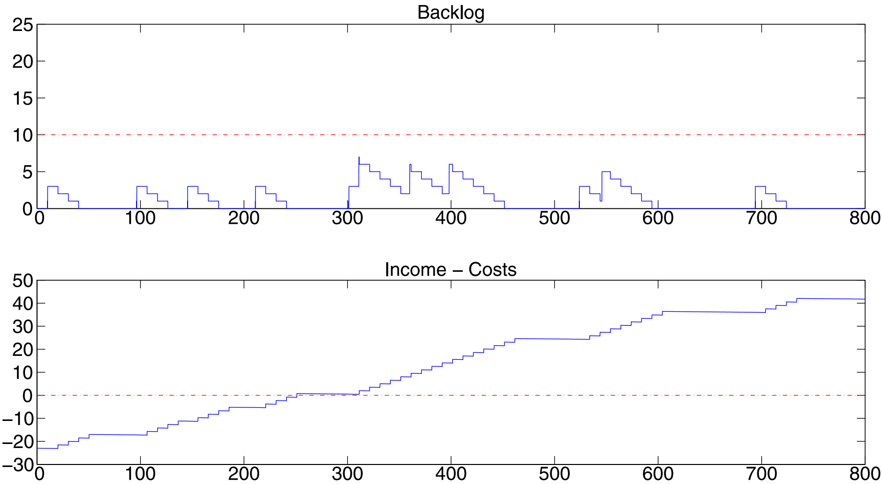


Fig. 6.15 Simulation result excerpt: silver level

- Simulation-based determination of additional costs, which are caused by this changing resource utilization. For instance, personnel have to be reallocated to guarantee the operability of a higher prioritized business process. As a consequence, the execution of the lower prioritized business process is disrupted leading to resources not working to full capacity.
- Simulation-based determination of resource requirements to minimize the impact of an occurred threat considering the shortage of resources resulting from downtimes of resources or insufficient resource capacities.

- Simulation-based identification of essential resources, which would cause severe backlogs of their dependent processes in case of reallocations.
- Simulation-based determination of additional resource requirements to eliminate backlogs caused by occurred threats.

All in all, in this section we outlined how our recently introduced concept of risk-aware business process simulation can be used to analyze security and economic viewpoints of business process. We believe that our approach brings significant benefits by using synergy effects of the business process, business risk, and business continuity domains.

6.6 Conclusion

The execution of business processes is the fundament of a company to meet its business objectives. These business processes are either support processes or directly provide aimed results (e.g., a product or a service for a customer). Business process management is the dominant domain aiming at optimizing the execution of business processes so that activities are performed efficiently and effectively in economic terms. “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” (Gartner Inc. 2009). However, business processes face threats that endanger the effective and efficient execution of their activities. There exist diverse classifications of these threats (National Institute of Standards and Technology 2002; BSI 2004; International Organization for Standardization 2004) ranging from accidents (e.g., unavailability of ICT resources or the absence of strategic personnel) to natural catastrophes (e.g., earthquakes), and to deliberate acts (e.g., sabotage or theft). The reasons why the execution of business processes may be affected causing negative effects on business are manifold and addressed by several domains. Traditional risk management—and thus implementations in according tools—considers risks on business process in a rather static way. Dynamic aspects are in fact only included through organizational risk management processes that let assessment be reperformed in certain intervals (e.g., biannually or annually). With our approach, we try to overcome this shortcoming and to use the advantage of dynamic business processes analysis when incorporating risk aspects leading to significant domain-overleaping synergy effects. Within this chapter we presented a reference model enabling the consideration of risks within business process evaluations based on our previously conducted research. Through the description of the requirements needed to enable risk-aware business process simulation, we are independent of graphical notation. As long as mandatory components and relations are considered, an evaluation is possible. Main benefits arising from the application of our approach comprise:

- Integrated modeling of business processes, risks, and detection, counter, and recovery measure information. Consequently, this allows the simulation of threats

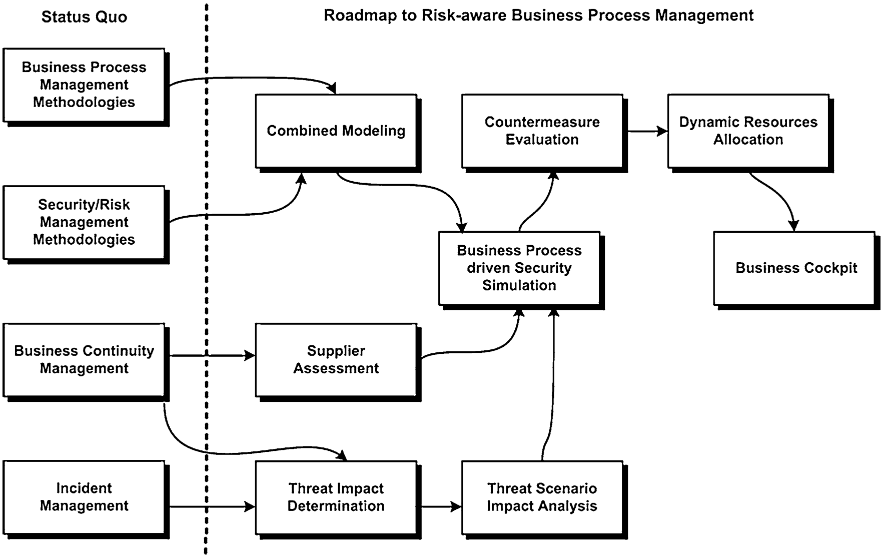

Status Quo
Roadmap to Risk-aware Business Process Management
Business Process Management Methodologies
Security/Risk Management Methodologies
Business Continuity Management
Incident Management
Combined Modeling
Countermeasure Evaluation
Dynamic Resources Allocation
Business Process driven Security Simulation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

Fig. 6.16 Roadmap to risk-aware business process management (Jakoubi et al. 2009)

and safeguard measures on attributes of business process elements, such as the availability or integrity of a resource. Subsequently, impacts on business process executions can be derived in a simulation-based way.

- Modeling and simulation of manifold scenarios to enable an evaluation of different security/contingency solutions.
- Identification of single points of failure or substantial weaknesses in resource planning and allocation. Simulation-based determination of resource requirements of business processes with regard to numerous threat scenarios.
- Provision of valuable information concerning the justification of security/ contingency investments when simulating different threatening and mitigation scenarios. Metrics such as the maximum tolerable period of disruption (MTPD) or mean time between failures (MTBF) can easily be determined. These may again serve as valuable input, e.g., for reviewing service level agreements.
- Simulation-based support of target-performance evaluations enhancing continuous process improvement cycles.
- Resource utilization strategies considering risks.

The presented formal model is a first step enabling the simulation-based evaluation of business process security. Figure 6.16 gives an overview about necessary steps towards comprehensive risk-aware business process management.

Giving a future outlook, the authors’ next research efforts will be laid in the inclusion of a dynamic reallocation of resources (e.g., for reducing backlogs caused by a threat’s impact) and in the in-depth consideration of service level management aspects leading to risk-aware service level planning and analysis.

References

F. Braber, I. Hogganvik, M.S. Lund, K. Stølen, and F. Vraalsen. Model-based security analysis in seven steps—a guided tour to the CORAS method. *BT Technology Journal*, 25:101–117, 2007.

British Standard Institute (BSI). British standard bs25999-1:2006: Business continuity management—part 1: Code of practice, 2006.

British Standard Institute (BSI). British standard bs25999-2:2007: Business continuity management—part 2: Specification, 2007.

BSI (German Federal Office for Information Security). IT-Grundschutz Manual (English version), 2004.

Business Continuity Institute. Good Practice Guidelines, 2008.

A. Ekelhart, S. Fenz, and T. Neubauer. Aurum: A framework for supporting information security risk management. In *Proceedings of the 42nd Hawaii International Conference on System Sciences (HICCS 2009)*, pages 1–10, 2009a.

A. Ekelhart, S. Fenz, and T. Neubauer. Ontology-based decision support for information security risk management. In *International Conference on Systems (ICONS 2009)*, pages 80–85, 2009b.

European Commission. Auditing directives. URL: http://ec.europa.eu/internal_market/auditing/directives/index_en.htm, Accessed May 2010.

European Network and Information Security Agency (ENISA). Business and it continuity overview and implementation principles, 2008.

S. Fenz, A. Ekelhart, and T. Neubauer. Business process-based resource importance determination. In *Proceedings of the 7th International Conference on Business Process Management (BPM2009)*, pages 113–127, 2009.

Gartner Inc. Gartner EXP worldwide survey of more than 1500 CIOS shows IT Spending to be flat in 2009, 2009.

G. Goluch, A. Ekelhart, S. Fenz, S. Jakoubi, S. Tjoa, and T. Mück. Integration of an ontological information security concept in risk aware business process management. In *41st Hawaii International Conference on Systems Science (HICSS-41 2008)*, page 377, 2008.

Gartner Inc. Misconceptions on process optimization and simulation. Gartner Blog, 2009.

International Organization for Standardization. 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, 2004.

International Organization for Standardization. Iso/iec 24762:2008 information technology—security techniques—guidelines for information and communications technology disaster recovery services, 2008.

S. Jakoubi and S. Tjoa. A reference model for risk-aware business process management. In *International Conference on Risks and Security of Internet and Systems*. IEEE, New York, 2009.

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*, pages 1596–1607, 2007.

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*, pages 1542–1554, 2008.

S. Jakoubi, T. Neubauer, and S. Tjoa. A roadmap to risk-aware business process management. In *Proceedings of the International Workshop on Secure Service Computing (SSC 2009)*, 2009.

A.K. Jallow, B. Majeed, K. Vergidis, A. Tiwari, and R.Roy. Operational risk analysis in business processes. *BT Technology Journal*, 25:168–177, 2007.

D. Karagiannis, J. Mylopoulos, and M. Schwab. Business process-based regulation compliance: The case of the sarbanes-oxley act. In *Proceedings of the 15th IEEE International Requirements Engineering Conference*, pages 315–321, 2007.

N. Milanovic, B. Milic, and M. Malek. Modeling business process availability. In *IEEE International Conference on Services Computing (SCC 2008)*, pages 315–321, 2008.

National Institute of Standards and Technology. NIST SP800-30, risk management guide fir information technology systems, 2002.

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

D. Neiger, L. Churilov, M. zur Muehlen, and M. Rosemann. Integrating risks in business process models with value focused process engineering. In *European Conference on Information Systems (ECIS 2006)*, 2006.

One Hundred Seventh Congress of the United States of America. Sarbanes–Oxley Act, 2002.

A. Rodríguez, E. Fernández-Medina, and M. Piattini. Towards a UML 2.0 extension for the modeling of security requirements in business processes. In *International Conference on Trust and Privacy in Digital Business (TrustBus 2006)*, pages 51–61, 2006.

S. Sackmann. A reference model for process-oriented IT risk management. In *16th European Conference on Information Systems*, 2008.

S. Sackmann, L. Lowis, and K. Kittel. Selecting services in business process execution—a risk-based approach. In *Business Services: Konzepte, Technologien, Anwendungen, Tagung Wirtschaftsinformatik (WI09)*, 2009.

S. Sadiq, G. Governatori, and K. Namiri. Modelling control objectives for business process compliance. In *5th International Conference on Business Process Management (BPM2007)*, pages 149–164, 2007.

The MathWorks. Simulink—simulation and model-based design, URL: http://www.mathworks.com/products/simulink/, Accessed May 2010.

S. Tjoa, S. Jakoubi, G. Goluch, and G. Quirchmayr. Extension of a methodology for risk-aware business process modeling and simulation enabling process-oriented incident handling support. In *Advanced Information Networking and Applications*, pages 48–55, 2008a.

S. Tjoa, S. Jakoubi, and G. Quirchmayr. Enhancing business impact analysis and risk assessment applying a risk-aware business process modeling and simulation methodology. In *International Conference on Availability, Reliability and Security*, pages 179–186, 2008b.

I. Weber, G. Governatori, and J. Hoffmann. Approximate compliance checking for annotated process models. In *1st International Workshop on Governance, Risk and Compliance—Applications in Information Systems (GRCIS'08)*, 2008.

M. zur Muehlen and M. Rosemann. Integrating risks in business process models. In *Australasian Conference on Information Systems (ACIS 2005)*, 2005.