universität
wien

DISSERTATION

Titel der Dissertation

Designing Business Continuity Response - A novel approach enhancing risk-aware business process management with dynamic resource allocation

Verfasser

Mag. Simon Tjoa

angestrebter akademischer Grad

Doktor der technischen Wissenschaften (Dr. techn.)

Wien, 2012

Studienkennzahl lt. Studienblatt:	A 786 880
Dissertationsgebiet lt. Studienblatt:	Informatik
Betreuer:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

Acknowledgments

> “ My best friend is the one who brings out the best in me.
>
> HENRY FORD

Finishing this thesis was one of my hardest scientific challenges in my career. Therefore, I would like to thank, in the following paragraphs, all those people who helped me to achieve this milestone.

First and foremost, I want to thank my family, especially my wife Bernadetta and my parents who were always supporting me.

I want to express my special thanks to my supervisors Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr and o. Univ.-Prof. Dr. Dimitris Karagiannis who always had an valuable advice or recommendation at the right time. Their guidance and support enabled me to finish this thesis. I would particularly like to thank Prof. Karagiannis for the possibility to use the OpenModels framework for this thesis, for the fruitful discussions we had and for his mentoring.

I would also like to acknowledge all co-authors of my publications - especially Stefan Jakoubi, Sigrun Goluch and Gerhard Kitzler - for all the numerous discussions, interest scientific disputes and support they provided me with during the time when I was writing this thesis.

Last but not least, I would like to thank all my friends and colleagues for their continuing encouragement.

Abstract

Companies are increasingly confronted with fast-changing risk-situations, leading to substantial challenges for business continuity and resilience professionals. Furthermore, the growing availability needs and the dependence on providers and suppliers demand an effective and efficient response to disruptions and interruptions in order to protect the brand, reputation and financial objectives of an organization.

As the preparation for 'expecting the unexpected' can be very costly, it is essential to highlight the benefits and advantages brought by proper business continuity planning. This thesis contributes to current research ambitions by presenting a formal approach extending the capabilities of risk-aware business process management. Risk aware business process management in general bridges the gap between the business process management, risk management and business continuity management domain. The presented extension within the thesis enables the consideration of resource allocation aspects within the risk-aware business process modeling and simulation. Through this extension it is possible to evaluate the effects of workarounds and resource re-allocations which is one crucial part in business continuity plans. In order to test the feasibility we implemented a prototype of our formal model using Simulink.

Additionally, in this work, we introduce a business continuity meta-model which is capable to capture essential business continuity requirements. The meta-model was implemented as a project within the OpenModels Initative.

Kurzfassung

Die rasch ändernden Risikobedingungen, mit denen sich Unternehmen heutzutage konfrontiert sehen, stellen Business Continuity und Resilience Verantwortliche vor neue Herausforderungen. Durch die zunehmende Abhängigkeit von Lieferanten und Geschäftspartnern sowie steigende Verfügbarkeitsanforderungen von Services wird es immer bedeutsamer, eine effektive und effiziente Reaktion auf Störungen und Ausfälle zur Verfügung zu stellen, um Ruf und Marke zu schützen sowie finanzielle Ziele zu erreichen.

Da die Vorbereitung und Planung einer Reaktion auf unvorhergesehene Ereignisse äušserst kostenintensiv sein kann, ist es notwendig, die Vorteile eines effizienten Notfallmanagements (Business Continuity Managements) nachvollziehbar zu begründen. Der in dieser Arbeit vorgestellte Ansatz erweitert das Konzept des Risk-Aware Business Process Managements, um Auswirkungen von Workarounds und dynamischen Ressourcenzuweisungen zu analysieren. Die Ergebnisse dieser Analyse dienen als signifikanter Input für die Notfallplanung. Für die Evaluierung des Ansatzes wurde ein Simulink Prototyp entwickelt.

Zusätzlich wird ein Metamodell zur Abbildung und Erfassung von Business Continuity Anforderungen, welches auf Basis der OpenModels Plattform umgesetzt worden ist, vorgestellt.

Contents

Part I

Background

Introduction

The journey of ten thousand miles begins with the first step.
Lao Tse

Events interrupting or disrupting business operations, such as natural disasters (e.g., earthquakes in Japan 2011 [6], closed airports due to Eyjafjallajoekull [87]), and targeted cyber attacks (e.g., Stuxnet 2010 [75]) are omnipresent in our media. "Whilst bombs, fires and floods capture the headlines almost 90% of business-threatening incidents are 'quiet catastrophes' which go unreported in the media but can have a devastating impact on an organisation's ability to function." [15, p. 5] These "quiet catastrophes" can occur in various ways. Examples [48, p. 4] are information security incidents, loss of utilities and services or deliberate disruption.

Is security aligned with business strategy and processes? What types of workarounds achieve the best results? How should the response to a disruption look like? What kind of cross-skill trainings are needed for whom? These questions play a central role in today's business life. However the answer to these questions is anything but simple.

The high relevance of the problem is also illustrated in a study by Knight and Pretty [73, pp. 3-5], who found out that there is a strong relationship between the incident response/business continuity and the shareholder value.

The reasons stated above are only a few indicators why Business Continuity Management (BCM) and Business Resilience (BR) are increasingly being used on a wider scale. [16, p. 4] [113, p.7] According to a study [114] conducted by the Chartered Management Institute (CMI), 84% of the companies that had activated their continuity plans agreed that they had reduced the impacts of disruption effectively. Possible sources for disruptions have been surveyed by [114]. The results for the time period 2002 - 2011 are shown in Table 4.1.

Table 4.1: Disruptions experienced 2002-2011 / Threats addressed by BCM 2011 [114, p.10]

	Disruptions experienced in previous years										Covered by BCM
	2002 %	2003 %	2004 %	2005 %	2006 %	2007 %	2008 %	2009 %	2010 %	2011 %	2011 %
Extreme weather e.g. flood / high winds	18	15	10	18	9	28	29	25	58	64	45
Loss of IT	19	24	25	41	38	39	43	40	35	34	52
Loss of people	-	26	20	28	29	32	35	24	28	34	35
Transport disruption	-	-	-	-	-	-	-	-	22	30	28
Loss of access to site	5	5	6	11	13	13	16	13	22	26	50
Loss of telecommunications	-	-	23	28	24	25	30	23	20	20	46
Supply chain disruption	19	11	12	10	10	13	12	9	13	19	26
Loss of key skills	33	16	14	20	19	20	21	14	15	18	30

School / childcare closures	-	-	-	-	-	-	-	-	18	17	12
Loss of electricity / gas	-	-	-	-	-	-	-	-	15	16	43
Employee health & safety incident	13	9	8	19	13	17	17	16	14	15	32
Negative publicity / coverage	24	17	16	17	16	19	18	14	9	11	20
Damage to corporate image / reputation / brand	15	7	8	11	8	11	10	11	7	10	24
Loss of water / sewerage	-	-	-	-	-	-	-	-	6	9	36
Customer health / product safety incident	11	6	4	6	6	6	7	4	6	7	24
Environmental incident	9	5	4	7	5	6	7	7	5	7	34
Pressure group protest	10	7	7	6	7	7	6	7	6	6	13
Industrial action	-	-	-	5	6	7	7	7	4	6	20
Fire	6	5	5	5	5	6	5	5	4	4	45
Malicious cyber attack	-	-	-	-	-	-	-	-	-	4	25

Terrorist damage	2	1	1	2	3	3	3	2	1	2	35

Although security is indispensable for every company to stay compliant with regulatory and legislative requirements, the utmost objective of every organization is to effectively and efficiently execute their processes to fulfill their vision and mission goals. While the visions and goals of every company vary, two characteristics remain stable. Firstly, business processes should be designed in a way that ensures commercial success, secondly, the executed tasks should be continuously available, protected against information security risks and compliant with the organization's governance requirements and standards.

A lot of work has been done to address both perspectives. However, most research focuses on solely one area. The business process perspective is mainly covered by process re-engineering approaches such as [68, pp. 81-106][70, pp. 10-13][96, pp. 376-389]. These approaches analyze processes to improve their design and to increase their level of automation. A tool that is often used to find potential improvements is business process simulation which enables the process architect to validate the design beforehand. When analyzing existing published work [64, 60], we have identified an essential shortcoming regarding the integration of security aspects which can play a crucial role in assigning resources. The reason for the importance of integrating security aspects is that requirements can change rapidly in the face of threats.

Security and continuity relevant aspects are mostly addressed separately. A very significant amount of time in different departments is spent carrying out tasks that ensure security and continuity. Disciplines and domains coping with these aspects comprise risk management [55, 80, 82, 83, 1, 23], business continuity management [10, 11, 14, 51, 79, 78, 24] and security incident/problem management [81, 112]. As in the process domain a lot of research efforts have been carried out in the last decades leading to a variety of different tools, techniques and approaches. However, a common reasoning and information framework that links both worlds is still missing. Therefore, we introduced a novel approach integrating a risk view into business process management which subsequently enables the simulation of risks within business process simulations [64, 60, 62]. This extension is the rationale of this thesis.

4.1 Problem Statement

Resources are the central element in every company to ensure that business operations and processes can be properly performed. Business processes and information are the key assets of every company. The intense global competition forces companies to economically optimize their business processes. For this reason there exist a variety of approaches and techniques to improve business operations. A well-established approach to improve processes regarding their efficiency is to perform business process management. The significance of this domain is highlighted by Gartner [41]. Driven by this need, approaches such as event-driven process chains [96, pp. 376-389] or the Business Process Management System [68, pp. 81-106] have been introduced and further developed.

Furthermore, regulatory and legislative requirements, such as SOX [88] and the 8th Audit Directive of the European Union [36], lead to growing demand for an integrated solution that combines compliance and security issues with business process management. A central element for the success of a company is the secure and continuous execution of their core processes and activities. According to the CA research report 'The avoidable cost of downtime' companies estimate that revenue is reduced by a third when business critical systems suffer an interruption. [17, p.2, p.8]. Another study of CMI (Chartered Management Institute) outlines in their BCM report that "over the past year, 40 per cent of organizations suffered disruption due to a loss of IT. Other key sources of disruption were extreme weather, loss of people, loss of telecommunications, and utility outages." [115, p.2]

Risk management, security management and business continuity management pursue the aim to achieve the objective of protecting information and ensure continuous operation within an organization. However, as the boundaries are fuzzy "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 crossover [...]" [37]

When combining these closely related disciplines with business process management, it gets even more difficult and complex, as different stakeholder groups such as decision makers, business process owners, re-engineering professionals as well as business continuity experts use different tools and techniques to fulfill their tasks. Consequently, there is no common language or well-established fully integrated approach that supports security and continuity aspects on the one side and the economic perspective on the other side. Another problem arises from the different perspectives of the disciplines. One such example is the operation of redundant resources. While redundant resources are highly recommended with respect to continuity aspects, it can generate a cost saving position from an economical viewpoint. This simple example already shows one challenge in the research ambitions related to business process security.

Currently, traditional business process management and simulation in general neglect the importance of the exchange of resources between processes during an incident (in the sense of IT contingency planning) to minimize the damage to a company. During an incident, however, this prompt re-allocation can make the difference between a successful and a failed response to an incident.

The research problem, addressed by this thesis, is therefore the question how to eliminate these shortcomings by integrating aspects of incident/business continuity management into business process management, thus leading to a novel and more holistic methodology. The following research questions should be answered by the thesis:

- How can a methodology and/or framework combine security disciplines (such as business continuity) with business process management?
- How can this framework improve the planning phase of business continuity and security incident management by evaluating dynamic allocations of resources? Which techniques are necessary to achieve this support?

The research questions in a broader sense pursues the aim to improve business continuity management systems(BCMS) by contributing to the evaluation of response processes and workarounds. Designing workarounds is one of the major steps of business continuity in order to diminish the negative effects of disasters and catastrophic events. The fact that the proper design of a workaround can decide over the existence of a company highlights the relevance of the problem.

4.2 Contribution and Research Approach

The objective of this thesis is to introduce the reader into the research field of risk-aware business process management which combines research elements from the domain of business process management, business continuity management, risk management and other security related disciplines.

The thesis presents the following main contributions:

- A literature review about the state of the art in the domain of business process security.
- A novel approach to integrate resource allocation perspectives into risk-aware business process management. The extension establishes a common model for business and security disciplines representing knowledge of both worlds as a basis to improve the decision basis for the planning of resource allocations as part of incident response planning.
- Design and implementation of a proof-of-concept-prototype in order to test the feasibility.

The interaction and interdependencies between business processes, activities and resources pose an enormous challenge. In order to overcome this complexity a modeling and simulation approach is used. In our approach activities are expressed by a completion function that determines how a task is accomplished. External factors such as threats can influence the functionality of resources or the execution of activities.

The selected research method comprises the following main steps and was influenced by the design research approach of [46].

The first step was to find a research problem with high relevance. For this reason an intensive effort was put into a literature review that analyzed the current state of research in the domain of business process security. The focus of the review was put on possible extensions regarding planning and design stages (phases with utmost relevance for researchers and practitioners in this area). After having formulated the research question, as immediate step thereafter, the approach was discussed with domain-experts at important international conferences.

As a next step, we identified requirements that should be fulfilled by our approach for evaluation and design purposes.

Within the design step, we solved two main challenges. Firstly, we developed a novel approach that supports the design and implementation of workarounds (in particular resource allocation) using risk-aware business process management. Secondly, we developed a meta-model and the architecture for our proof-of-concept prototype to suit the theoretical framework.

In the implementation phase we realized the meta-model using the OpenModels platform [71]. We decided to use Simulink for simulation purposes.

In the evaluation we modeled a simplified sample business process derived from a real world example in order to show the applicability of the approach. Furthermore, we presented our approach at various conferences and workshops to disseminate our method ([64, 60, 43, 102, 104, 62, 101]) and to get feedback about the method.

4.3 Terminology

In this section we cover some important terms related to risk and business continuity management in order to clarify their usage within his work.

Risk

"The combination of the probability of an event and its consequence." [54] For information security risk the ISO27005 [55] refines this definition by adding the vulnerability component. "Potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation"[55] In this thesis the definition of [54] is predominantly used. However, when it comes to the consideration of threats, countermeasures and their interdependencies related to business process activities the definition of [55] helps to get a deeper understanding.

Risk Assessment

"A process used to identify and evaluate risks and their potential effects." [52]

Risk Management

"Risk management is a systematic approach for minimizing exposure to potential losses. It provides a disciplined environment for

- continuously assessing what could go wrong (i.e., assessing risks)
- determining which risks to address (i.e., setting mitigation priorities)
- implementing actions to address high-priority risks and bring those risks within tolerance

"[2, p.6]

Resilience

The National Institute of Standards and Technology (NIST) defines resilience as "the ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning."[98]

Business Continuity Management

The London Resilience Team defines business continuity management as planning to ensure that an organization “[...] has a relatively quick and painless return to ’business as usual’ in the event of a major disruption.”[74] This brief and simple definition highlights a central element of this thesis, namely the planning factor to prevent business from suffering irreversible damage. This planning stage should be improved through the analysis of dynamic resource allocations within risk-aware business process management. A more comprehensive definition can be found in [99] which states that “Business Continuity Management (BCM) is a holistic process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause. It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities.” [99]

The Australian Prudential Standard APS 232 summarizes all essential aspects of BCM in a nutshell. ´´Business continuity management (BCM) describes a whole of business approach to ensure critical business functions can be maintained, or restored in a timely fashion, in the event of material disruptions arising from internal or external events. Its purpose is to minimise the financial, legal, reputational and other material consequences arising from the disruption.”[3]

Business Process

Weske [111] defines business process as “... a set of activities that are performed in coordination in an organizational or technical environment ...”[111, p. 5] The execution of activities is performed to achieve business goals and objectives. Furthermore, processes have the ability to interact with each other. [111]

Business Process Management

Business Process Management includes according to [111] “... concepts, methods and techniques to support the design, administration, configuration, enactment and analysis of business processes.”[111, p. 5]

Business Process Re-engineering

The essential phases of a re-engineering process can be found in [68, 106]. Tsalgatidou and Junginger highlight in their work [106] the following four sub-processes within the re-engineering process: *Goal Definition, Information Acquisition, Modeling and Evaluation*. The phases of the operational model presented in [68] introduce the following core tasks within the re-engineering phase: *criteria selection, information acquisition, analysis, design, evaluation and implementation*. Figure 4.1 schematically outlines the operational model of the re-engineering process.

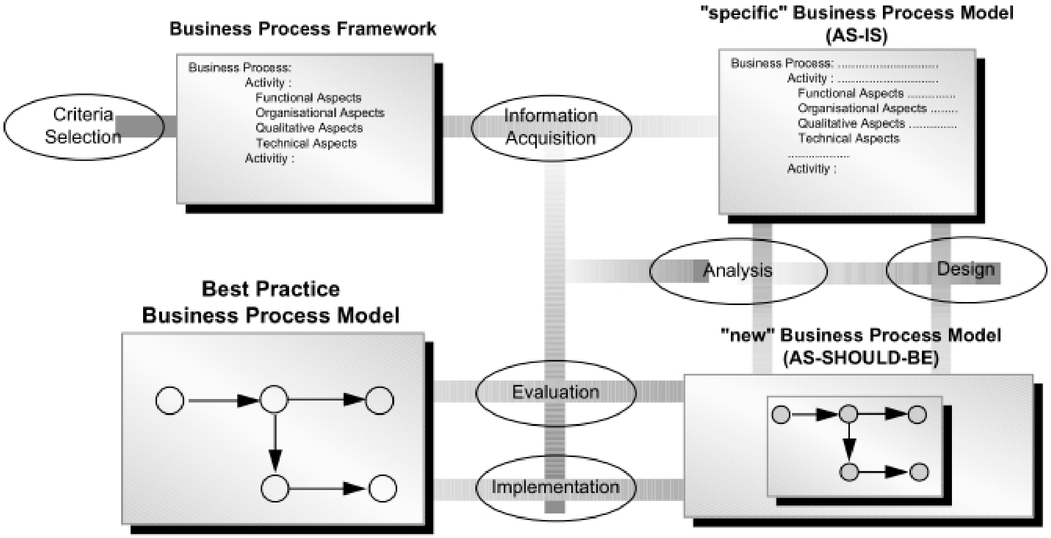

Business Process Framework
Business Process:
Activity :
Functional Aspects
Organisational Aspects
Qualitative Aspects
Technical Aspects
Activity :
Criteria Selection
Information Acquisition
"specific" Business Process Model (AS-IS)
Business Process: ....
Activity : ....
Functional Aspects ....
Organisational Aspects ....
Qualitative Aspects ....
Technical Aspects
....
Activity :
Analysis
Design
Best Practice Business Process Model
"new" Business Process Model (AS-SHOULD-BE)
Evaluation
Implementation

Figure 4.1: Re-engineering Process [68]

4.4 Structure

The core parts of this thesis are structured as follows: Chapter 5 highlights related research approaches that are of high importance for this thesis. It outlines fundamental approaches in the domain of modeling and simulation of business processes as well as scheduling patterns for workflow and business process management. Chapter 6 introduces our approach to risk-aware business process management. This approach integrates risk aspects into business process management which allows us to consider economic and security perspectives simultaneously.Furthermore, it highlights the extensions of our approach in order to support the analysis of workarounds (Section 6.3 - Section 6.6). These extensions enable effective response planning through the simulation of resource allocation effects. Chapter 7 outlines our prototype architecture before the results of our approach are discussed. Chapter 8 describes the meta model of our risk-aware business process management approach including the extension regarding resource allocations. The last chapter of this thesis (Chapter 9) concludes this work and highlights open resource questions.

Parts of this thesis have been excerpted from the previously published papers [64, 43, 102, 60, 104, 58, 62, 61, 63, 101, 103]. The chapter 6 of this thesis is partly co-written with Mag. Stefan Jakoubi [59] as the contents of these parts have been derived from jointly written papers [64, 43, 102, 60, 104, 62] and describe our approach to risk-aware business process management which is the foundation of this thesis.

The major contribution of this thesis is the significant extension of risk-aware business process management in order to facilitate the planning phase of business continuity and security incident response through risk-aware resource management. This novel approach aims at the efficient and effective re-allocation of resources at the re-engineering stage in order to improve the planning and evaluation of (business continuity and incident) response processes. The possibility to visualize the workarounds, beside simulating them for improvement purposes, enables reuseability for simplified emergency procedure flow charts in business continuity documents.

Through the approach presented in this thesis we want to achieve better senior management commitment by showing the business case for implementing an adequate response. Furthermore, we aim to raise a deeper understanding about the value of business continuity.

Related Work

> “If you wish your merit to be known, acknowledge that of other people.
>
> ORIENTAL PROVERB

Within this chapter we outline related research in our area in order to highlight how our research efforts relate to other approaches and concepts. Furthermore, the following sections should provide new readers a good overview of recent developments in the domain of business process security, dynamic resource allocations with focus on business process and workflows and business process resilience as well as business continuity.

5.1 Approaches Integrating Risks and Security Aspects in Business Process Management

This section provides information about related research in the domain of business process security. The majority of the presented approaches in this section integrate or combine risk, business continuity, security or dependability aspects with business process management aspects.

Sackmann identifies in his paper [94] the following challenges for traditional risk management methods. The dynamic nature of IT implies a lack of experience regarding the relation between IT risk and implications of changes. The relations between IT and business processes are often complex. An occurring risk on one IT system can have effects on several business processes. [94, p. 3] In order to face the challenge, the author introduces a layer-based IT risk reference model (Fig. 5.1 containing the following layers [94, pp. 4-6]:

1. Business Process Layer (Layer 4 / BP Layer): In this layer it is important to model the business processes that should be considered. The author emphasizes that for further analysis steps, it is essential to determine the monetary contribution of a process to the company's results.

2. IT applications / IT infrastructure layer (Layer 3 / AP Layer): Supporting IT applications as well as their underlying infrastructure components are included in this layer.

3. Vulnerabilities layer (Layer 2 / VN Layer): This layer captures the vulnerabilities of IT applications and their infrastructure components. This enables a bridging of IT threats to business processes.

4. Threats layer: this layer contains information about all known threats. If possible, the information about threats should include their probability of occurrence.

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” [94]. For expressing these relations (i.e. the searched cause-effect relations) a matrix-based description is used.

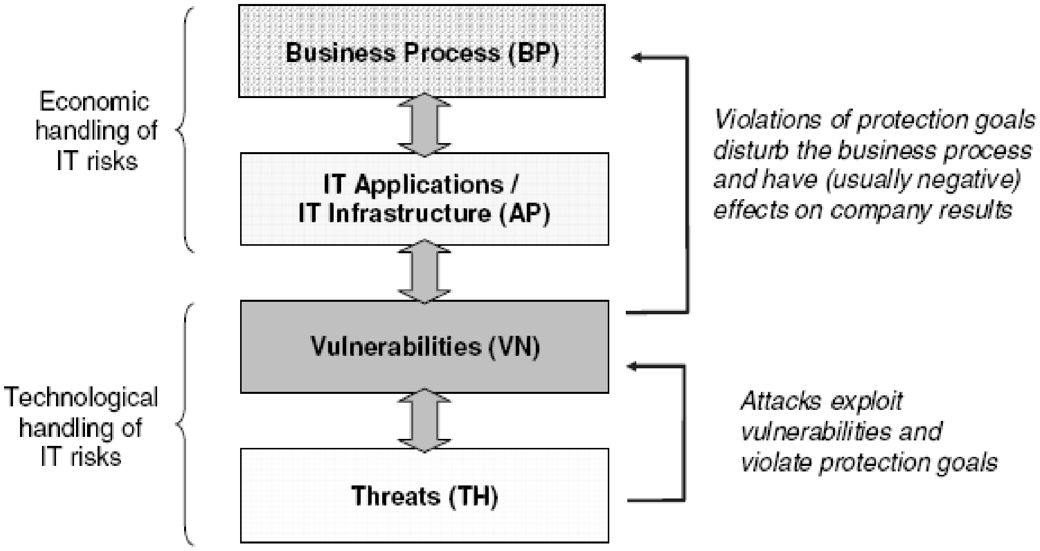

Economic handling of IT risks
Technological handling of IT risks
Business Process (BP)
IT Applications / IT Infrastructure (AP)
Vulnerabilities (VN)
Threats (TH)
Violations of protection goals disturb the business process and have (usually negative) effects on company results
Attacks exploit vulnerabilities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

Figure 5.1: IT Risk Reference Model [94]

In their work zur Muehlen and Rosemann highlight the strong connection between processes and risk. On the one hand, risk management is a process, on the other hand risks have to be considered in business processes for various reasons. The authors also stress that research in both domains is based on different methodologies and is conducted by different groups with different focuses. [119, pp. 1-2]

According to the authors, besides a common understanding of business processes, two important aspects have to be considered: Firstly, there exists a link between objectives and processes. Processes can be refined into activities. As risks can be linked to activities too, risks can also be seen as goal-sensitive. Secondly, a process is more than just a flow of activities. Thus, other risk-sources such as incoming business objects, data, resources or IT are relevant for risk management activities. They therefore, introduce in their paper a taxonomy for business processes containing the *clusters goals, structure, information technology, data and organization* as well as the two distinguished lifecycles *build-time and run-time*. Further a risk taxonomy (Fig. 5.2) is introduced which enables consideration of process risks. [119, pp. 3-5]

In order to adequately capture the risks they propose the following four model types [119, pp.

5-8]:

1. Risk Structure model: In this model a hierarchy of risks is represented. For modeling risks two types of relations (i.e. part-of and is-a) are used.

2. Risk Goal model: This matrix-based model provides information about the impacts of risks on the goal of an organization.

3. Risk State model: This model captures dynamic aspects of risk. The main modeling types of the model are risk, consequence and connectors.

4. EPCs extended with risks: This model enables the analyst to link individual activities to specific risks.

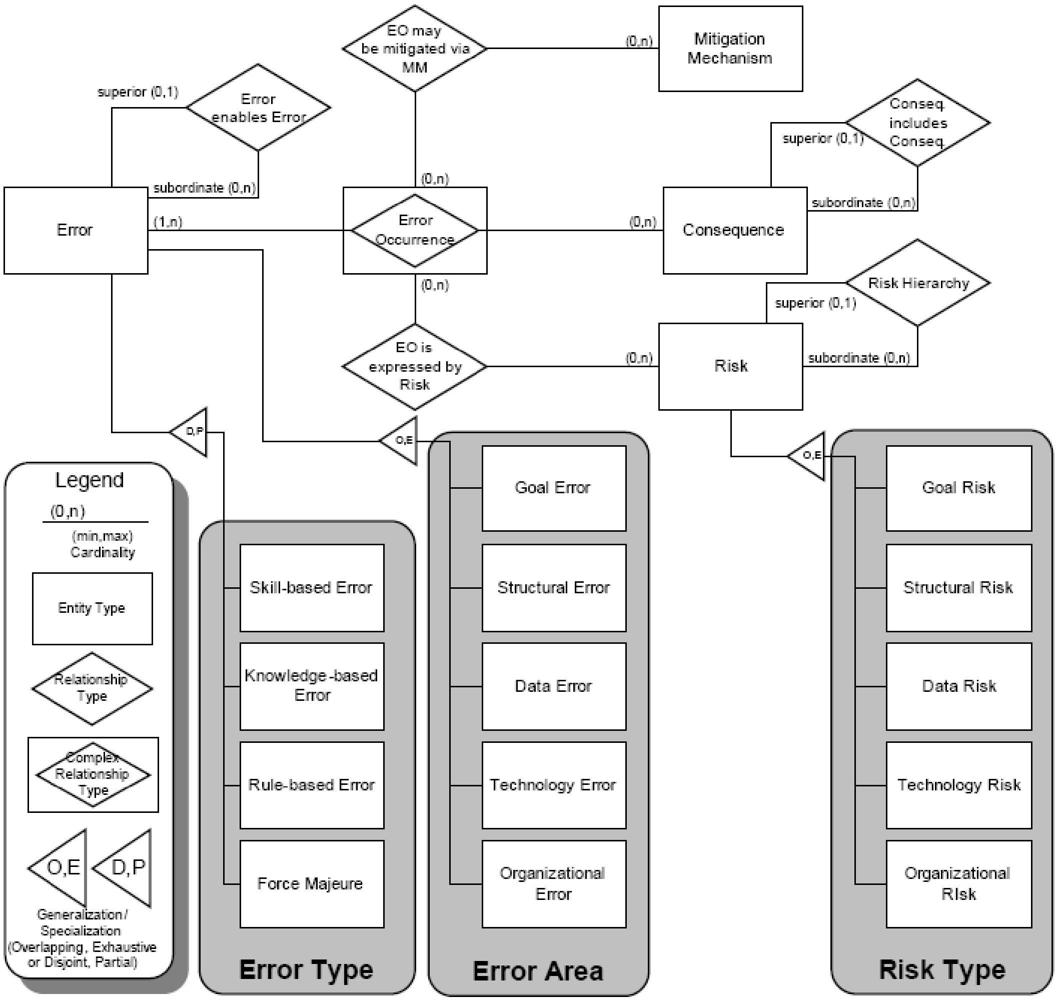


Figure 5.2: Risk Taxonomy [119, p. 4]

In their paper [85], Neiger et al. stress the need for a holistic business view on risk management. The authors therefore, introduce a conceptual framework to bridge the gap between process management and risk management. The underlying foundations for this conceptual framework build the risk oriented process management introduced by zur Muehlen and Rosemann [119] and the concept of value-focused process engineering introduced by Neiger and Churilov [84]. Both approaches use event-driven process chains as a basis. [85]

The link between value-focused process engineering and risk management is established through the consideration of risk treatment as a business objective. The four steps to enable a proper integration are [85]:

- Decomposition of business values and fundamental objectives in order to identify relevant process risks.
- Value focused principles are used in order to identify specific risks. An articulation of links between activities and risk-related objectives takes place. The result is a link between objectives and the process flow.
- Identification of alternative process configurations that fulfill the business objectives
- The alternative configurations and their corresponding outcomes are compared in order to select the optimal process configuration (meeting the risk objectives)

[8] is a UML-based approach for conducting security risk analyses. Figure 5.3 outlines the conceptual model of the CORAS approach. The methodological process supporting the CORAS approach consists of the following seven steps:

1. Introductory meeting: This step focuses on determining the goals of the analysis and on gathering information about the target.
2. High-level analysis: In a separate meeting, the analysis team presents their understanding of the information provided in the initial step. Furthermore, a high level security analysis is conducted in this step which comprises the identification of "... threats, vulnerabilities, threat scenarios and unwanted incidents ..." [8, p. 101] The output of this step is used to improve scoping and to ensure that the direction of the next analysis steps is appropriate.
3. Approval: Within this step the description of the target is refined. Further, assumptions and predictions are captured. The steps ends with an approval of the information by the client.
4. Risk identification: In a workshop threats, vulnerabilities as well as unwanted incidents and threat scenarios are identified by people with expertise on the evaluation target.
5. Risk estimation: In this step the information is refined by providing estimates about the likelihood and consequences of unwanted incidents.

6. Risk evaluation: A risk picture is presented in this step in order to trigger possible adjustments and corrections.

7. Risk treatment: Through a workshop treatment and cost / benefit issues are identified.[8]

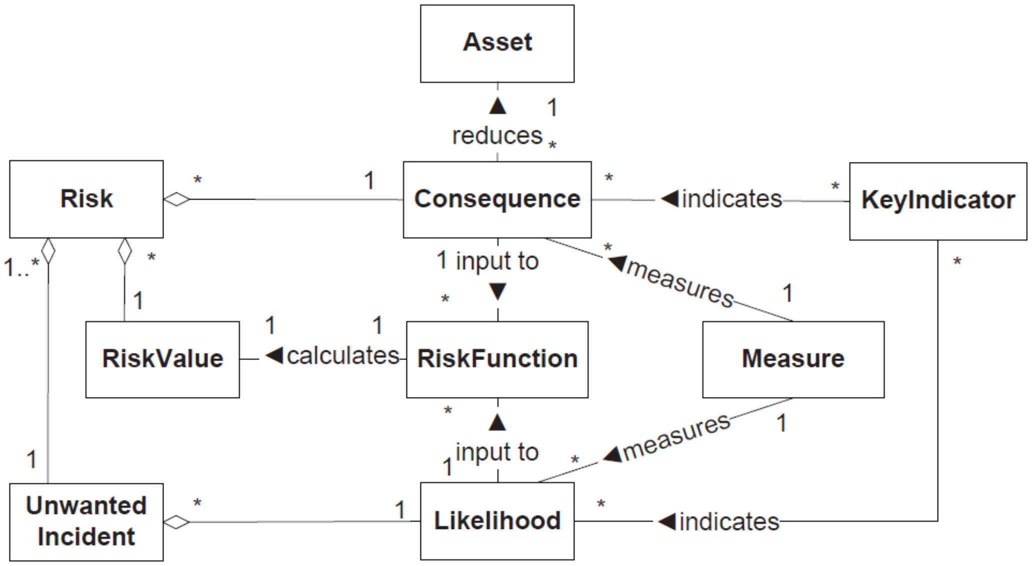


Figure 5.3: CORAS conceptual model [90]

Karagiannis et al. [69] introduce in their paper a business process based approach supporting reporting requirements of the Sarbanes Oxley Act (SOX) . The approach contains six steps and is realized in the professional toolkit ADONIS®. In order to enable their compliance extensions (i.e. requirements demanded by SOX [88] and COSO (Committee of Sponsoring Organizations of the Treadway Commission) [25]), the ADONIS® standard modeling language has been extended .

The presented framework contains the following steps [69, pp. 318-320]:

- Business Process Acquisition: The central element of the approach are business processes. For this reason, the acquisition of business processes takes place in the initial step. The authors highlight that it is important to provide detailed information in order to get good results.

- Risk Management and Scoping: In this step accounts significant to SOX are identified and documented in a 'Significant Account Model'. Further, related risks are identified, documented and modeled. For each risk the likelihood and impact is determined. Through the tool used for this assessment, the impact of the risk situation is immediately shown by a traffic light coding. This evaluation is the starting point for determining controls.
- Design Effectiveness: This stage "... deals with the revision of internal controls, intended to balance risk and control costs ..." [69].
- Operating Effectiveness: In this step controls are analyzed with respect to their effectiveness. Depending on the results different remediation measures may be applied.
- Internal Management Review: In this step it is evaluated whether the company is SOX-compliant. The evaluation report is then signed-off by management.
- Auditor's Final Review: In the last step an external auditor who is independent receives the financial reports and internal management review report.

The approach was evaluated in a case study with a US insurance company covering nearly 200 business processes. For more information we refer the reader to [69].

Sadiq et al. present [95] another approach to support business process compliance. In their paper the authors highlight the need for systematic approaches to understand the interconnection and dependency between business and control objectives. Accordingly, the authors present an approach that enables the modeling of control objectives using the Formal Contract Language (FCL) which was introduced in [44]. For visualization in the process models the authors use 'process annotations'. A sample process (simplified purchase-to-pay scenario) clarifies how the approach can be applied to existing processes.[95]

Sienou et al. present in their paper [97] a method for the integrated management of process risk, including a lifecycle model, a metamodel, a modeling language and a set of usage rules. Furthermore, the authors identified the following challenges originating from the different viewpoints of risk and business experts: (1) Incompatibilities in the organization structure of risk management and process management (2) Semantic incompatibilities of risk and process related information. In order to overcome the before-mentioned challenges the authors propose the following approach: (1)

Synchronization of process management and risk management lifecycles (2) Incorporation of risks and processes in one holistic meta model (3) Operational developments of languages and rules.[97]

Rodriguez et al. [91] propose in their paper a UML 2.0-based approach to model security requirements of business processes. The extended UML activity diagram serves business analysts to specify their security requirements. In a second step security analysts complement the specification of the business analysts. Figure 5.4 outlines the extended activity diagram meta-model.

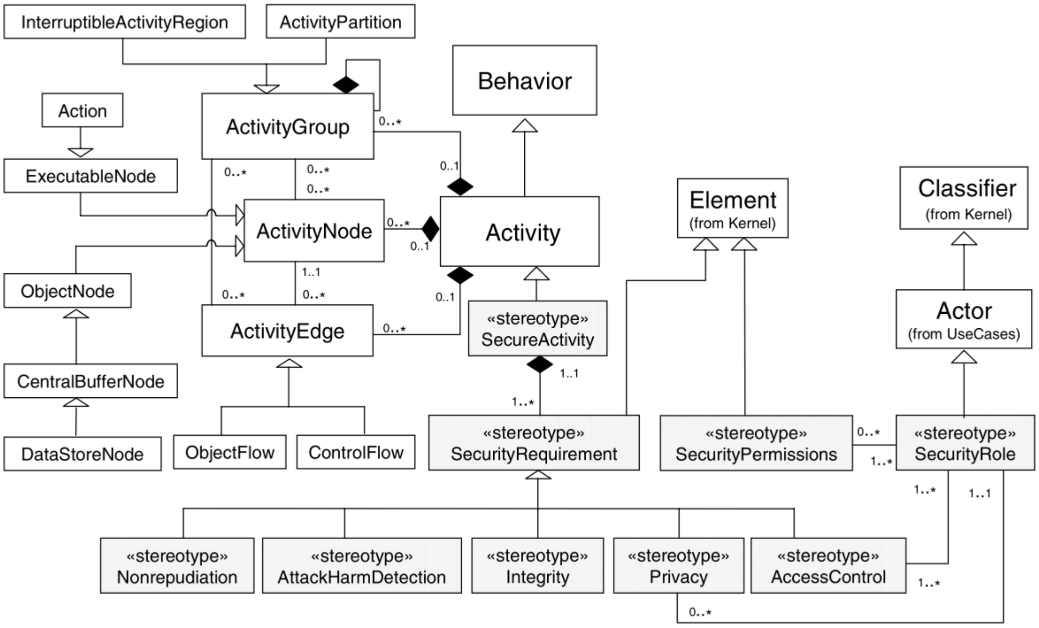


Figure 5.4: Extended meta-model with security stereotypes [91]

Weber et al. [110] propose another approach to validate processes against compliance requirements. The basis for their approach is a set of constraints. This constraint base enables compliance check with regard to the following two scenarios: (1) checking new or altered processes (2) checking all processes against altered compliance requirements.

Jallow et al. [65] propose a framework for risk analysis in business processes which mainly focuses on the identification and analysis phase. As a basis for their risk assessment dimensions the authors use the criteria cost, time and performance/quality as proposed by Zhou and Chen [118].

The framework follows the six steps of Figure 5.5, i.e.:

1. Model the activities and risks of the business process: In the first step the *activities* of a process are modeled. In the subsequent steps, *risks* are firstly evaluated on activity level and thereafter analyzed on process-level.

2. Determine the objectives: As described above, three dimensions (i.e. cost, time and output) are used for the evaluation of a process. For the analysis of an activity, the authors suggest the same dimensions. As their current approach only allows one dimension at a time, the evaluation objective should be determined in this phase.

3. Identify risk factors, probability of occurrence and impact: In this phase, risk identification takes place. While identifying the risk, the probability of occurrence is determined as well.

4. Define assumptions (regarding the risk impact): In this step, assumptions are drawn about the possible impacts of a risk. As the authors claim that it is difficult to determine a single value, they decided to use a three point estimate (consisting of a *low* impact case, the *most likely case* impact and the *worst case* impact) resulting in a triangular function to describe the risk impacts.

5. Calculate risk: For each risk factor the risk output is determined by multiplying the occurrence rate with the impact magnitude. ”The impact is not a discrete value but a series of values generated by the simulation based on the distribution” [65].

6. Calculate forecast: The framework supports two types of forecasts. One for each activity and a accumulative forecast for the whole process.

In order to test the framework, the authors implemented a prototype using Microsoft Excel and the add-on software Crystal Ball™.

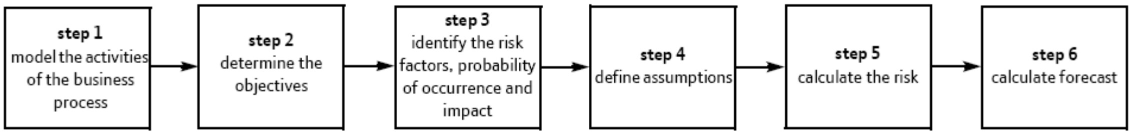


Figure 5.5: The risk-based proposed framework [65]

Breu et al. [9] present in their work a systematic IT risk assessment approach for enterprises and projects. The basis is an enterprise model which either exists or has to be created. This enterprise model is structured in the following three levels or views: (1) business level (2) application level (3) technical level. The usage of the model facilitates the evaluation of dependencies between the different layers. [9]

Regarding the security management process the authors extended typical security management core actions (i.e. *elicitation of security requirements*, *identification of threats*, *evaluation of risks* and *countermeasures engineering*) in two ways. Firstly, for the security analysis process, a meta-model is introduced to perform all core actions in the context of enterprise model elements and secondly, the core process is a security micro-process continuously performed on the enterprise model. Figure 5.6 outlines the activities of the security micro-process and figure 5.7 the security information meta-model[9].

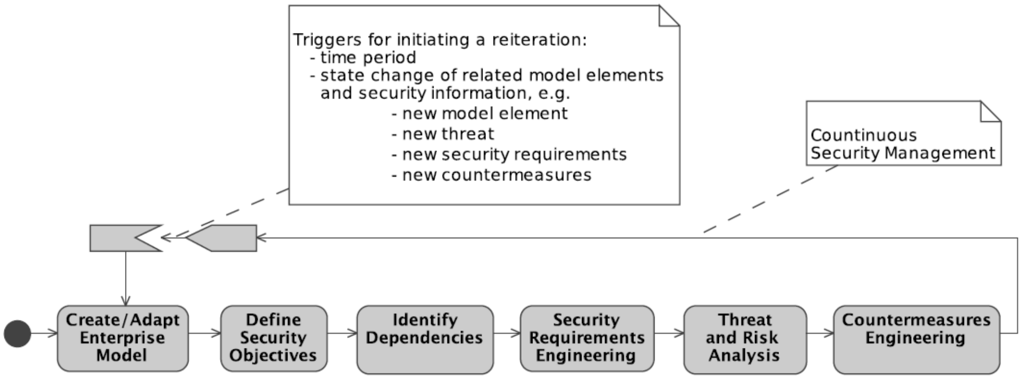

Triggers for initiating a reiteration:
- time period
- state change of related model elements and security information, e.g.
- new model element
- new threat
- new security requirements
- new countermeasures
Countinuous Security Management
Create/Adapt Enterprise Model
Define Security Objectives
Identify Dependencies
Security Requirements Engineering
Threat and Risk Analysis
Countermeasures Engineering

Figure 5.6: Security micro-process [9]

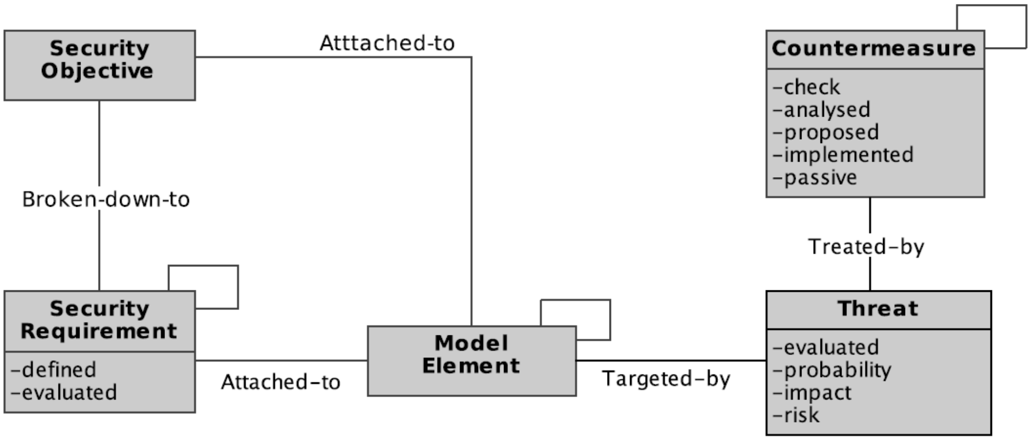


Figure 5.7: Security information meta model [9]

AURUM is a framework for automated information security risk management [31, 39, 32, 40]. The authors identify the following questions which have to be considered by every organization[40]:

- What are potential threats for my organization?
- How probable are these threats?
- Which vulnerabilities could be exploited by such threats?
- Which controls are required to most effectively mitigate these vulnerabilities?
- What is the potential impact of a particular threat?
- What is the value of security investments?
- In which security solutions is it worth investing?

Fenz et al. [40] focus on the development of concepts providing answers to the above-mentioned questions. Furthermore, they pursue the objective to provide support for risk managers in order to improve security decision making. The specification of the developed concepts introduces new risk management approaches and techniques on a conceptual level and constitutes the basis for further tool implementations. Fig. 5.8 highlights the supported ISRM-phases. The aim of the framework is to support decision makers in order to select security solutions in an efficient and effective way. [31, 39, 32, 40]

The approach consists of the following phases: (1) Business Process Importance Determination, (2) Inventory Phase, (3) Threat Probability Determination, (4) Risk Determination and (5) Control Identification and Evaluation.

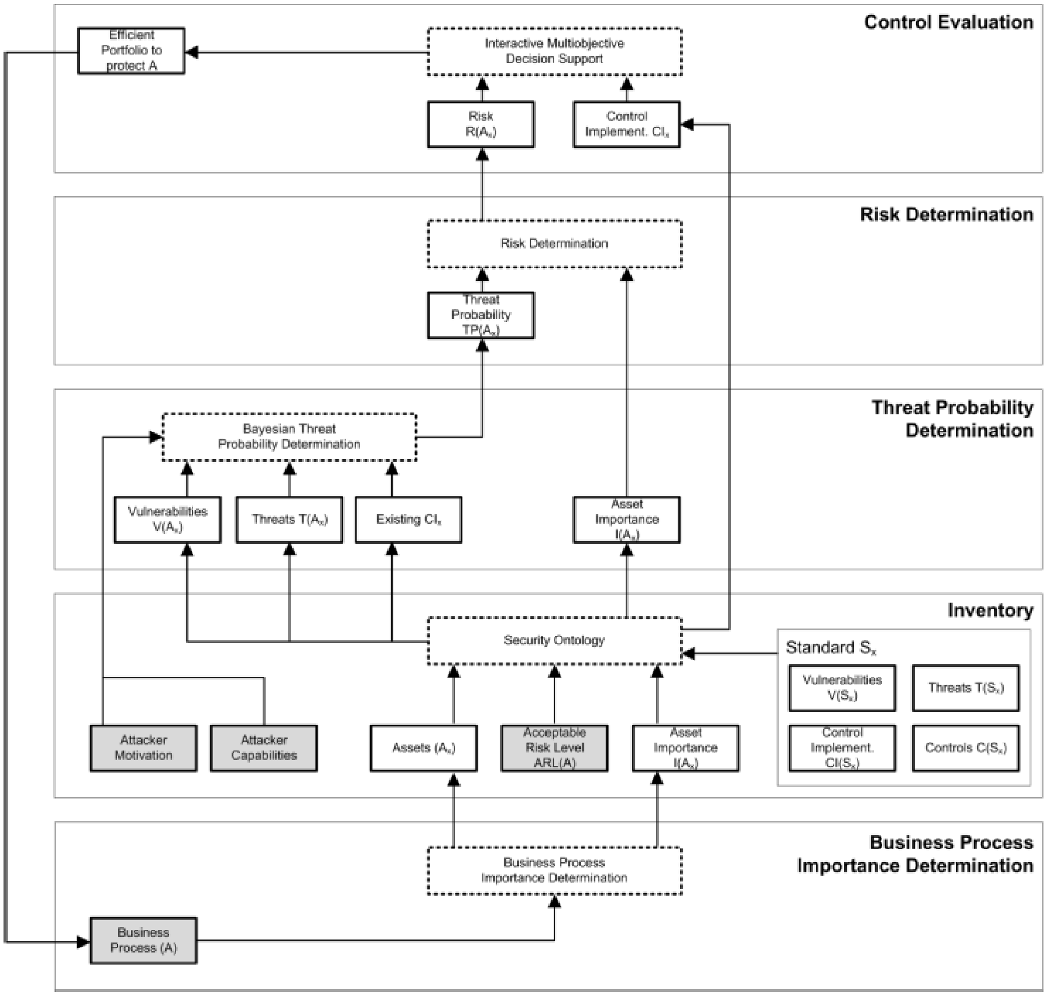

Control Evaluation
Efficient Portfolio to protect A
Interactive Multiobjective Decision Support
Risk R(A_x)
Control Implement. CI_x
Risk Determination
Risk Determination
Threat Probability TP(A_x)
Threat Probability Determination
Bayesian Threat Probability Determination
Vulnerabilities V(A_x)
Threats 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)

Figure 5.8: The AURUM process [40]

Jensen et al. [66] present a novel approach to incorporate security specifications and model driven software development. Therefore they introduce an EPC Security Model View which is implemented as new perspective within the ARIS SOA architect.

Figure 5.9 illustrates the architecture proposed by the authors. An EPC model view is supplemented by EPC Security Model View which is used for security requirements specification. The specifications are used when generating the WS Security Policy and BPEL processes at a later stage. At the moment of creation, the work was still in progress. Thus, the authors concentrated on prioritized security properties such as access control, confidentiality and integrity.

The security model used to specify security requirements, consists of standard EPC notation and the four security symbols: (1) message level encryption, (2) signature, (3) end-to-end encryption, (4) access control. To ensure that no business requirements are negatively affected by the security view, it is not allowed to change any EPC element out of the EPC security model view. EPC components that need not be analyzed within the security perspective have a gray filling.

After all security requirements are modeled, the requirements can be realized by using a fully automated transformation procedure described by the authors. According to the authors, the usage of EPC is not compulsory as their concept is language-independent.

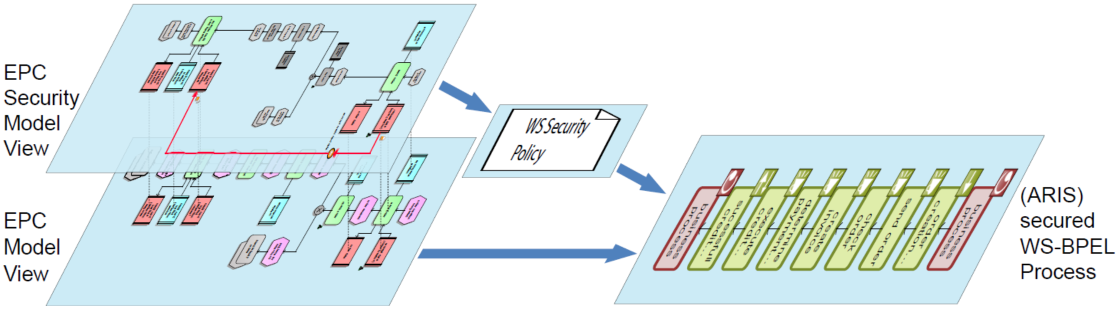


Figure 5.9: An example view principle for event-driven process chains in the ARIS SOA Architect [66]

5.2 Dynamic Resource Allocation within Risk Aware Business Process Re-engineering

In the following paragraphs we briefly outline essential information about resource allocation and scheduling.

Effective and efficient planning / scheduling of resources as well as considering tasks' interdependencies are crucial for reacting on critical incidents. [22]

Aalst et al. also outline in [108] the importance of dynamic resource re-allocations: ´´The idea of resource redeployment is to increase the capacity of the resources associated to cases or tasks that are running late. Resource redeployment can take many forms including: adding more resources (e.g., moving people between departments), extending the scope of the roles associated with a task (e.g., allow people with a lower role to execute the task), increasing the capacity per resource (e.g., overtime) or changing the allocation of tasks to achieve load balancing." For further escalation mechanisms and resource allocation patterns such as task pre-dispatching or resource re-deployment, we refer the reader to [93, 108, 92, 47].

The use case for scheduling algorithms and approaches is manifold. Whenever it comes to considerations to optimize time and resource utilization scheduling plays an important role. Examples where this discipline can provide valuable input comprise production scheduling for manufacturers, course scheduling for schools/universities or time tables for transportation services.

"In the offline shop scheduling problems such as job-shop, flow-shop and open shop problem, each job contains several steps (tasks) and all jobs are known before scheduling. So that, many optimization algorithms such as Neural Network and Generic Algorithm can be applied to find out an optimized scheduling plan. In the online non-shop scheduling, each job contains only one step and jobs arrive over time. So that, rules based algorithms are employed, such as SRPT (Shortest Remaining Processing Time) and SJF (Shortest Job First)." [109]

As within our risk aware business process management approach jobs, resources and even tasks (e.g. activity allocation) can vary due to uncertainty originating from risks, we concentrate in the following on those rule based algorithms that currently provide the best results. However, as the research domain of scheduling is a very active field, our conceptual model as well as the prototypical implementation allow easy replacement of the algorithm used. For more detailed information on scheduling algorithms we refer the interested reader to detailed evaluations of scheduling algorithms such as [89]

The scheduling approach used within our evaluation example is based on the principle of prioritization. The reason for this choice is simple: Incident response, recovery and continuity procedures are normally strictly prioritized in order to enable an effective and efficient response in the case of an emergency. [57, p. 16] One result of our literature review is that this can be best achieved by this concept.

Another interesting aspect that is derived from the generalist - specialist problem is that we assume that resources can replace other resources to full or partial extent. In the following we shortly introduce the challenge and the way Netjes et al. solved the problem.

Netjes et al. [86] introduce an approach addressing the challenge of the specialist-generalist trade-off and the flexible assignment policy. The specialist-generalist trade-off has the objective to identify the optimal ratio between specialists which are capable to perform one task and generalists which can perform more than one task.
Furthermore, it is assumed that specialists can do their task faster than generalists. The usage of the flexible assignment policy should guarantee that the best possible flexibility is preserved for the future. This implies that if two resources for a task are available (one specialist and one generalist), the specialist will be assigned with a higher priority to carry out the task to maintain a better flexibility. Within the scope of the paper, business processes consist of inter-related tasks. A task is carried out by one resource. A task has the restriction that it can either be fully performed or not at all. Resources have different roles to facilitate the mapping between resources and tasks.

For modeling and analyzing such a resource-constraint process, the authors use colored petri nets (CPN). Within these CPNs tasks are connected to generic resource modules which contain the role capable to fulfill the task. The allocation strategies that can be used by resource modules to assign resources to tasks are priority-based or random. If the priority based allocation strategy is used, pre-defined priorities are used to allocate the resources. In the second case, resources are allocated by randomly drawing a resource that is capable to perform a task out of the resource pool. In order to illustrate the approach, the authors present a short sample bank process modeled in CPN using their allocation approach.[86]

Korvin et al. present in their work [26] how tasks can be assigned to resource pools. A task can have certain requirements and each pool provides resources with mixed capacities. The significance of a resource for executing a specific task is determined via its membership. The membership value is a number between 0 and 1, where zero indicates the lowest importance level (no use) and a one indicates the highest importance or dependency. [26]

Xu et al. [116] pursue a similar direction. They analyze the usage of resources in order to significantly reduce costs of the business process execution through a more efficient allocation of required resources. Therefore, they introduce their concept of a role-based business process model which defines resources, roles, tasks, business processes and their relations in order to enable an appropriate determination of the most cost-effective resource allocation.

If neglecting the cost factor, Topcuoglu et. al[105] propose an earliest-finished-time algorithm to optimize the processing time of processes.

Both pools (i.e. task pool, resource pool) are organized as finite fuzzy sets. In the case of a resource pool, the membership attributes indicate the pool's possibility to provide resources. For example, a membership value of zero states that the pool is not able to provide the needed resource. Korvin et al. derive a so called measure of compatibility between task and resource pools. This compatibility is also organized as fuzzy set. The center of area method is used to enable a comparison of the sets' defuzzifications. Furthermore, an algorithm is described how to recursively assign tasks to resource pools and to handle violations (i.e. no assignment possible). For decision making purposes, the authors consider costs of using a pool and a flexible budget (the initial budget limit may be exceeded to some extent if the need is accordingly large). To reflect importance issues, the approach allows the weighing of compatibility and costs.[26]

5.3 Business process resilience and business continuity

Zalewski et al. suggest in their work [117, pp. 113-125] business processes to model disaster recovery plans. They highlight that the analysis with automatic tools has enormous advantages compared to manual analysis. A further benefit of using a modified business process notation, besides the graphical and uniform representation of information, resides in the possibility to check the validity of the model. To model business continuity and disaster recovery plans the authors suggest the following layers: Organizational View, Data View, Functional View, Product/Service View and Process/Control View. The authors successfully used their model to analyze the DR plan of the University of California. [117]

Boehmer et al. [7] present an approach to analyze business continuity plans using process algebra and modal logic. Within the paper they clarify their approach with a simplified loan process. [7]

Khanmohammadi and Houmb present in their paper [72] an approach to evaluate information security by using process-based information. The idea behind the approach is that assets only pose value to an organization or individual if they are used within a process or task. In order to better evaluate the state of risk, they separate processes into business process and control processes. Control processes are all processes that protect business processes or assets such as encryption or access control. [72]

Caralli et al. present in their paper [19] the CERT® Resilience Management Model (RMM). The model uses foundational concepts including services (set of activities), business processes (set of discrete activities or tasks contributing to service mission), assets (everything of value for a company) and resilience requirements. The RMM is further structured into 26 process areas containing practices that facilitate improvement of resilience in the specific area. [19] Detailed information about the resilience model can be found in [18], [20]

Dey [28] briefly outlines in his paper the importance of business continuity. Furthermore, he outlines the essential components that are necessary to perform business continuity. For further information on relevant professional guidelines and standards, we kindly refer to [42].

5.4 Chapter Summary

In this section we gave an insight into existing concepts, methods and techniques in related research areas of this thesis.

In the first section we introduced various approaches, which has achieved the following results:

- Specification of security requirements
- Reduction of the gap between business process management and risk management
- Extended evaluation capabilities regarding business process availability and compliance

All mentioned approaches in section 5.1 made significant contributions in the field of business process security. However, to our knowledge no approach exists so far that is able to incorporate risk and security aspects into business process management and provides support for the planning and evaluation of workarounds in order to improve the organization's resilience.

In the second section we outlined various publications considering resource scheduling in business processes. We presented various different approaches used in the research field of scheduling. As in *nearly all* business continuity plans a comprehensive prioritization exists we concentrated on *scheduling by priority*. However, as a requirement of this section the meta-model presented in this thesis also incorporates the possibility to include other scheduling techniques.

In the last section of this chapter we provide a short overview on the topic business continuity management and resilience which sets the background to the thesis. We highlighted approaches which are currently trying to combine business processes and continuity efforts.

Part II

The Methodology

Risk-Aware Business Process Management

> “Nothing is more difficult than the art of maneuvering for advantageous positions.
>
> SUN-TZU

In this section, we present the main idea behind risk-aware business process management [64, 102, 104, 60] in order to both provide the reader with an adequate overview and to clarify our contribution in the following sections.

In our vision, risk-aware business process management can be ideally performed when building appropriate bridges between business process management and the relevant security domains (e.g., risk or business continuity management). As the logical next step, *risk-aware business process modeling* consequently enables adequate simulations. These two techniques are the cornerstones of business process planning and reengineering where our current research focus lies.

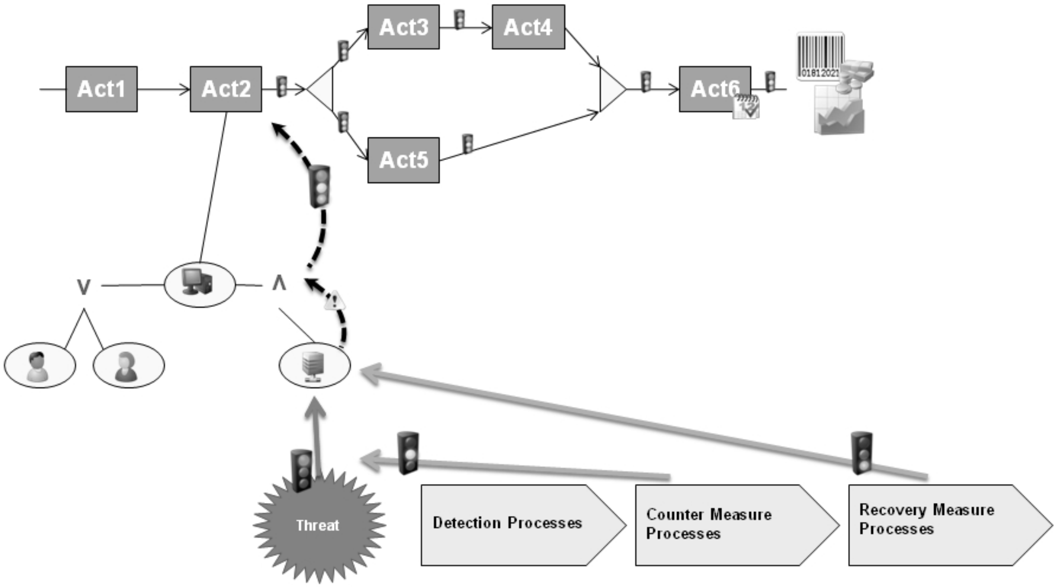


Figure 6.1: Conceptual Approach towards Risk-Aware Business Process Modeling and Simulation

In a nutshell, in our conceptual approach (see Fig. 6.1) business process elements, such as activities and resources, are endangered by threats. If a threat is successful, one of the possible impacts may be the unavailability of a resource, leading to delays in the execution time of connected activities. In order to represent the current security situation detection-, counter- and recovery measures are modeled. If sufficient information is available, these measures are modeled as business processes that require resources and are endangered by threats. Detection measures invoke counter- and/or recovery measures. The quality of the measure affects the point in time when detection or invoking respectively, takes place. Counter measures try to eliminate an occurred threat and recovery measures try to re-establish the functionality of potentially affected business process elements. Basically, detection measures are the first step and thus can influence counter and recovery measures, whereas the efficiency and effectiveness of counter measures only influence following (or overlapping) recovery measures. Fig. 6.1 shows the conceptual approach described above. In our opinion, it is a real strength of our approach that results of typical projects, such as business process analyses, risk assessments or business impact analyses, do not end up as dusty reports in cabinets but can be modeled and subsequently used in a continuous manner or simulation purposes.

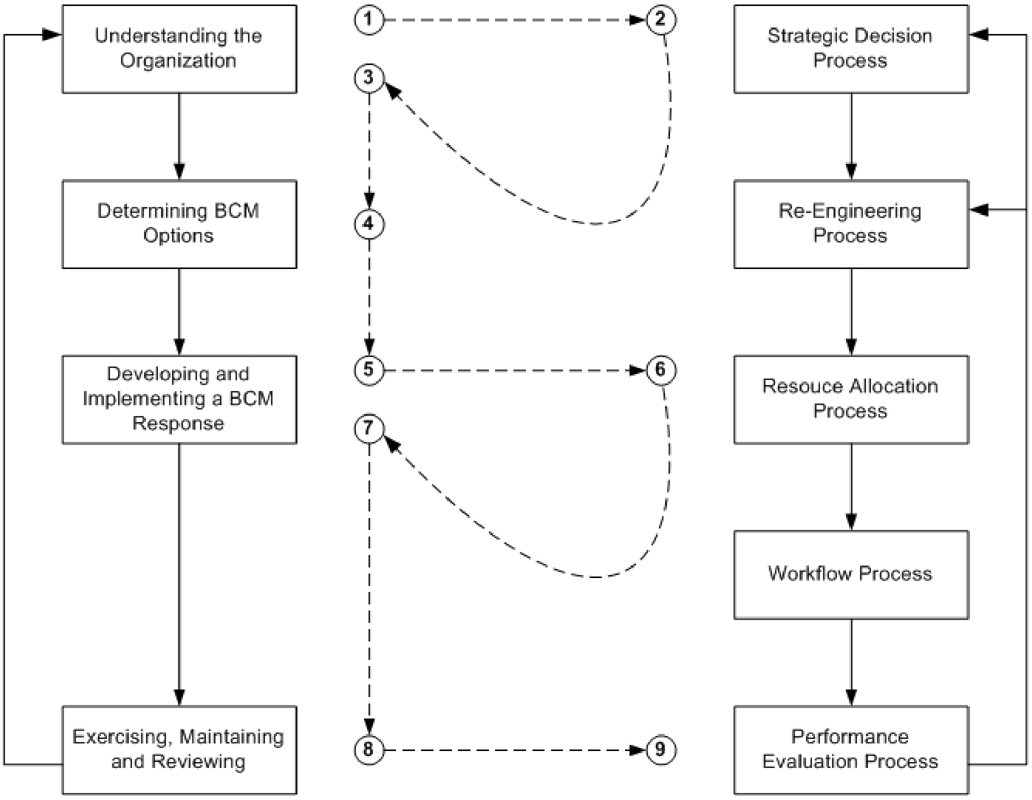

Understanding the Organization
Determining BCM Options
Developing and Implementing a BCM Response
Exercising, Maintaining and Reviewing
1
2
3
4
5
6
7
8
9
Strategic Decision Process
Re-Engineering Process
Resouce Allocation Process
Workflow Process
Performance Evaluation Process

Figure 6.2: Introduction of Risks into Business Process Management

Consequently, we further concentrate on our vision of building the bridge between business process management and risk as well as contingency domains. To exemplify our vision, Fig. 6.2 schematically depicts core activities of the Business Continuity Management (BCM) Life Cycle (left side) according to [10, 11] and core activities of the Business Process Modeling paradigm BPMS (right side) according to [68]. Our bridging concept is sketched in Fig. 6.2.

Important steps and issues to integrate the above mentioned domains and concepts are:

1. The interconnection of business process modeling and simulation techniques together with

business impact analysis and risk assessment techniques enables the risk-aware business process analysis.

2. Processes can be much better understood by not only focusing on economic factors, but also by taking risks and business process activity disruptions into consideration. Financial and reputational impacts of a process interruption, for example, should definitely be taken into account when defining strategic guidelines, success factors and essential criteria (e.g. availability requirements) for the business processes of a company.

3. This broadened view delivers added value when (re-) engineering and optimizing the business processes. Subsequently, prospective business processes which have been designed under consideration of economic, continuity and risk information will be available.

4. Consequently, this delivers added value for determining BCM options as the evaluations of potential strategies (e.g. alternate data center) are tightly aligned to the available business process information (e.g. product/service value, processes' prioritization or availability/recovery requirements).

5. Selecting the most appropriate option is the basis for developing and implementing the BCM response. Accordingly, plans can be developed considering specific process characteristics such as minimal resource requirements after an incident.

6. Risk-aware designed business processes and their related continuity plans build the foundation for determining appropriate resources. This comprises not only resource utilization considerations to perform the business process activities under normal conditions. When a threat occurs, which endangers the activities' execution, it will trigger the invocation of plans that detail the steps to be taken during and after an incident (to maintain and restore operations).

7. This further leads to a sufficient integrated implementation of both, the business process execution in the operation environment and the institution of the business continuity and business recovery plans.

8. The aggregation and preparation of process information, extraction of performance indicators and metrics serves as valuable input for iterations in the BCM life cycle.

9. Lessons learned and metrics from plans’ rehearsal or even invoked plans trigger again the start of a process to continuously improve the understanding of a company’s business and its processes.

6.1 Steps Required to Perform Risk-Aware Business Process Management

This section outlines essential steps of the proposed approach in order to conduct risk aware business process management. The steps are derived from several best practice documents, guidelines and standards in business continuity, security and risk domains. However, although we aligned the approach with existing frameworks/standards and recommendations, they should be understood as a valuable toolbox (reflecting the state-of-the-art in this topic) and not as rigid or inflexible requirements. As a complete and comprehensive BCM guide would go far beyond the scope of this work, we refer to dedicated BC literature such as [29, 16, 10, 12, 34, 13] in order to get a comprehensive view on all mentioned topics.

Figure 6.3 provides an overview on the different phases (Perform Program Management, Determine AS-IS Situation, Re-Engineer Processes, Implement Process, Review and Evaluate) of our conceptual approach.

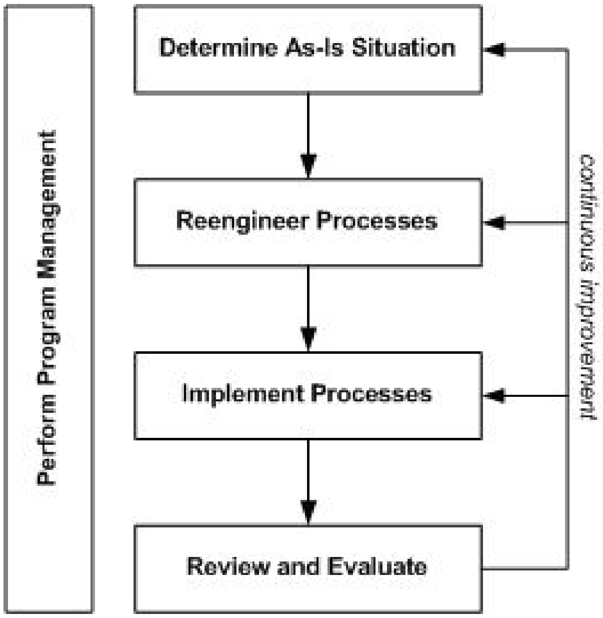


Figure 6.3: Recommended Phases for Performing Risk-Aware Business Process Management [62]

6.1.1 Perform Program Management

The program management is responsible for ensuring that all projects and activities in the scope of risk-aware business process management are carefully planned and controlled. This component is a key function as inadequate program management most often results in additional costs, delays and a decrease in quality.

We will now discuss key activities that should be carried out in order to provide good program management for risk-aware business process management.

Scope Definition

The definition of the scope is crucial to ensure that the program meets its objectives. It is good practice to clearly define and document the scope in order to ensure traceability. Typically, a scope definition indicates which business units, functions and processes are subject to the program. Other criteria, such as geographic scale or products, can also be used to define the scope.

When deciding on a scope, one should be aware of the fact that a too narrow scope definition can lead to misleading results, as important parts of an organization could be out of scope. On the other hand, a too widespread definition can waste considerable amounts of money.
In order to guarantee the adequacy and correctness, senior management should sign-off the scope. As the environment of a company can change dynamically, the scope should be evaluated at least annually.

Organizational Environment

Within this step, information is collected about the environment in which the company operates. This includes information about customers, competitors, shareholders and other stakeholders. Furthermore, it is important to clearly specify and analyze the vision, mission and business objectives of a company in order to understand the strategy and tactical decisions.

The results of this key activity contribute to a clear understanding of the organization, which is crucial for evaluating risks and countermeasures. Deficiencies in the understanding of the objectives and strategies of an organization obviously will lead to inappropriate continuity measures.

Risk and Continuity Evaluation Criteria

Only a goal that is correctly and comprehensively specified can be achieved. For this reason it is important to introduce criteria in order to measure the outcome of a program. When defining these criteria one should consider that the metrics are specific, measurable, attainable, relevant and time bound (SMART) as described by [76].

Examples of such measurable criteria would be a cost reduction by five percent in the next quarter or a service availability of at least 99 percent in the next year.

Besides the above-mentioned evaluation criteria, consistent criteria for risk, safety and security evaluation activities should be defined. These criteria should include at least:

- which impacts (e.g. financial, brand, reputation, health, compliance to regulations and laws) should be considered
- which scales should be used for measuring impacts. Some examples can be found in [38, p.9]
- which scales should be used to rate the criticality of services, resources or processes (e.g. highly critical, critical, normal, low, negligible)
- the approach to evaluate risks and business impacts (e.g. usage of a qualitative or quantitative approach)
- which residual risk is acceptable for the organization for which impact category

As in the previous steps, the best way to manifest all the important criteria is their formulation in formal documents which have a reliable document control. This will enable the traceability of decisions on countermeasures.

In order to plan workarounds and dynamic resource re-allocations, re-allocation criteria should be determined. These criteria include information such as when resource allocations should take place, to which extent resources should be re-allocated or what social and cultural aspects should be considered concerning human resource allocations.

Roles and Responsibilities

The set up of a successful program always requires a clear definition of roles and responsibilities. For business continuity programs it is recommended to have at least a sponsor at senior management level. As various assessments are required to obtain the desirable results appropriate resources should be assigned to the program.

Furthermore, it should be mentioned that for an effective BC response it is inevitable to have an adequate communication and escalation structure. Various standards and guides (e.g. [16, 12]) provide helpful information on this topic.

Program Steering

The program coordination team is usually responsible for monitoring and controlling the program activities. This typically includes project management activities such as time and budget management, resource management, quality management as well as program risk management.

6.1.2 Determine As-Is Situation

An evaluation of the current situation regarding security, risk and continuity is essential to plan further steps. In order to support organizations, we recommend to perform the following steps.

Core (Business) Process Identification

The first step when using our approach is to determine the core business processes. As these processes strongly contribute to the success of the organization and ensure the continuity of the organization, information should be collected carefully. All business units within the scope should be surveyed to guarantee that sufficient information about the core activities, execution paths and dependencies is gathered.

The information about the business processes should be mapped to the organization's goals. Furthermore, details should be acquired about each process (activity) such as costs and execution times as well as the contribution of the processes (e.g. monetary value, intermediate products). Apart from that, internal and external dependencies and interdependencies should be documented.

Resource Identification

Resources are required in order to perform all activities. Therefore, required resources, their interdependencies and their assignment to activities are determined in this step. The skills, knowledge, financial value and other resource properties such as geographic dispersion or replacement costs have to be acquired in order to enable further analysis steps. Current metrics and security for resources such as recovery time objectives or recovery point objectives have to be gathered.

Furthermore, rules for resource allocation have to be created. These rules require the following information: Firstly, one has to assign a resource map that outlines which resources can be re-allocated or replaced by which resources and to what extent. Secondly, rules have to be provided that indicate when a resource is re-allocated at the current situation (i.e. thresholds for certain attributes).

Risk Identification

In order to cope with risks, it is important to deeply understand them. Therefore, in this step techniques such as described in [56] are used to identify risks. The overall objective is to get a list of risks the company is confronted with. Threat and hazard lists can constitute valuable input for this task.

Using risk-aware business process management at least the following two types of risks should be considered during risk identification [62]:

- 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.
- 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 disasters from meteorological institutes or information security trends from research organizations.

Detection, Counter and Recovery Measure Identification

This step delivers information about implemented countermeasures and safeguard processes. In order to safeguard an organization, different tasks are required. Firstly, a threat has to be detected in a timely manner to ensure a successful response. Examples of such detection measures are fire detectors or other alarm systems. In our model it is possible to consider internal and external mechanisms. Depending on the detection method, counter- and recovery measures may vary. In order to clarify why this step is necessary, we want to give the following example. If a fire detector that is coupled with a sprinkler detects a fire, the sprinkler will immediately try to extinguish the fire. However, if a pedestrian detects a fire, he or she will likely call the fire brigade.

In our approach we categorize counter measures into two categories:

- Preventive counter measures: A preventive counter measure is a measure that changes the probability of occurrence of a threat (e.g. non-smoking policy)
- Reactive counter measures: In contrast to a preventive measure, a reactive measure decreases the potential impact by fighting a threat after it is detected (e.g. fire suppression system).

The last type of measures that should be identified within this step are recovery measures. These measures recover resources and re-establish their functionality. An example of a recovery measure is the restoration of data with back-up tapes.

The acquired information is represented according to the proposed model, which enables further analyses such as risk-aware business process simulations as have also been introduced in our previous work [64, 43, 102, 60, 104].

6.1.3 Reengineer Processes

This phase pursues the aim to simultaneously improve business processes considering security, continuity and economic viewpoints. When identifying options, it should be mentioned that business goals and requirements have to be the key driver. A security or continuity solution should always be cost-effective (i.e. the benefit of the measure exceeds the costs/impacts).

By establishing the link between counter measure and business process we strongly contribute to more transparency. With this ability we are also capable of fulfilling the requirement [53, pp.46-47] to track controls to business demands. Measures which cannot be traced back to a business need should be further investigated, analyzed, and questioned.

In order to improve the continuity of the processes within an organization, at least the following phases have to be performed.

Business Impact Analysis
The business impact analysis (BIA) is the key-component of every business continuity program. It is a powerful tool to evaluate relevant dependencies (e.g. key supplier) and to analyze impacts over time. The focus of the analysis lies on activities that are mission critical. Mission critical activities are activities that are time-critical to the organization (i.e. a disruption of such an activity causes critical damage in a short time span such as a few hours).

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). [14]

In the course of this work, a metamodel is presented that can be used to capture the information required to conduct a business impact analysis. As an additional advantage, valuable information can be generated through simulations as described in [64, 43, 102, 60, 104].

Risk Analysis
The risk analysis evaluates identified risks regarding their occurrence probability and their impact on resources and/or activities. Furthermore, interdependencies between risks (see [4]) as well as the effects of existing and planned countermeasures should be analyzed. The outcome of this phase is a list of threats that should be addressed as the residual risk is not acceptable (according to the company's risk strategy and criteria).

For detailed information about risk analysis, we refer the interested reader to dedicated risk management literature ([21, 2, 4, 56, 55, 77])

Identification of Improvement Options

The identification of areas for improvements is the key objective of this phase. An important aspect within this step is that security improvements should always be evaluated from a security *and* economic point of view. Another outcome of this activity is the prioritization of improvement alternatives. For this task it is vital to have clear criteria how prioritization should take place.

The resource re-allocation approach described in this thesis offers a new opportunity to identify, evaluate and assess various improvement options by demonstrating the effects of workarounds through the simulation of dynamic re-allocation of resources (and activities).

The set of improvement options should be documented and presented to the senior management for sign-off. This ensures that the implemented improvements comply with organization's objectives and strategies.

Redesign of Processes

Once the decision is taken, which opportunities for improvement should be realized, the redesign activity starts. Within the redesigning processes, special attention should be drawn to existing best practice process structures and key controls such as separation of duties. The usage of risk-aware business process simulation can be used to thoroughly test business process designs at an early stage.

Evaluation

As widely known, planning and design errors become more and more expensive at later stages. For this reason, in the evaluation step the process designs are evaluated against the pre-defined criteria. Any deficiencies found in the evaluation lead to a new process iteration. This ensures that expensive design errors are minimized. Furthermore, lessons learned should be documented to ensure continuous improvement.

6.1.4 Implement Processes

This step is the main driver for introducing the new process designs. The restructuring and redesign of processes is a challenging task. For this reason it is important to consider at least the following topics in order to successfully perform the changes. A successful implementation will pave the way for effective and efficient processes.

Project Setup

Due to the obvious advantages, it is highly recommended that process changes are implemented by individual projects. Through the set up of projects it is easier to have a good cost control. An important point to note is that clear roles and responsibilities for the projects should be assigned. Furthermore, clear cost and time constraints should be defined.

More information about project management activities such as project controlling, staffing or risk management can be found at [50].

Implementation

In this phase it is important to analyze and evaluate several technical solutions supporting the design of the new processes. A further critical success factor is the adequate communication of process changes in order to improve acceptance. If necessary, awareness trainings should be performed to improve the organizational security / continuity culture.

The implementation phase can last for a longer period of time depending on the approved (budgeted) scope of the implementation projects. For projects with an estimated duration longer than one year, it is recommended to introduce controls and intermediate milestones (e.g. every n months) in order to facilitate project management and control. A project status evaluation should be carried out at least once a year.

Evaluation

The continuous improvement of processes is a vital requirement for organizations in order to be competitive and successful. Therefore, in this step deficiencies, identified in the stage, are investigated, analyzed and documented. Depending on the significance of the problem a new iteration (i.e. a project remediating the problem) is started.

6.1.5 Review and Evaluate

Deming [27] highlights the particular importance of continuous improvement of products and services. Feedback loops (as Shewhart cycle [27, p. 88] or helix [27, p. 181]) are an integral part to improve the quality of any system.

Business continuity, risk management and business process management are strongly influenced by dynamic factors. Therefore it is important to review and control the processes on a regular basis in order to ensure that changes in risk situations, market environment and other significant aspects are recognized in a timely manner. Testing of business continuity and security capabilities of an organization is indispensable in order to guarantee an effective response to incidents.

6.2 The Formal Model

This section outlines our novel formal model. The mathematical model presented in this section provides the capability of modeling business process elements (such as activities and resources), threats, safeguards, their dependencies and interdependencies as well as impacts. In our current approach, we only consider the security attributes availability, confidentiality and integrity. However, the formal model can be easily extended to consider further attributes such as dependability attributes proposed by Avizienis et al. [5].

6.2.1 A Formal Description of Business Process Elements

We define business process elements as those components that are necessary to describe a business process and its dependencies as well as interdependencies within our model. Within our model $\mathcal{P} := \{process_1, \ldots, process_k\}$ represents the set of all possible business processes within an organization.

Each process can further be broken down into more granular components such as activities and resources. In our model, we therefore introduce $\mathcal{A}ct = \{Act_1, \ldots, Act_l\}$ as the set of activities and $\mathcal{R} = \{R_1, \ldots, R_n\}$ as the set of resources.

In our formal model, we further define the following assumptions: Each activity Act_i possesses, one exact set of assigned resources AsR_i and one activity assembly $As(Act_i)$ (assumption 6.1). Each process ($process_j$) is structured in a similar way. This means, for each process $AsAct_j$ (assumption 6.2) one exact set of assigned activities exists.

$$\forall Act_i, i = 1, \ldots l : \exists! AsR_i \land \exists! As(Act_i) \tag{6.1}$$

$$\forall process_j, j = 1, \ldots k : \exists! AsAct_j \tag{6.2}$$

In order to characterize the business process elements presented above we introduce the set of attributes $\mathcal{A} = \{A_1, \ldots, A_m\}$. Therefore, all processes, activities and resources have their own set of attributes out of set $\mathcal{A}$.

The resources required to perform an activity are expressed by RR_i, where the index *i* represents the corresponding activity. Within RR_i, information is provided which attributes of a certain resource are required to execute an activity. In order to clarify our idea Fig.6.1 graphically outlines this condition.

Formally described, tuples of the form $RR_i := \{Act_i; \{(R_j, A_m, Z_j, f_{j,m}(t)), \ldots | R_j \in AsR_i\}\}$ can be used, where Act_i is the specific activity, R_j represents a resource, A_m its required attribute and Z_j the threshold indicating the minimum level of an attribute (e.g. availability = 100%) that is required to perform an activity. If the attribute falls below Z_j (e.g., threat impact) and no redundant resources are available, then the corresponding activity is impacted. The function $f_{j,m}(t)$ describes how the alteration of the resource's attribute condition changes the activities' condition itself. Through the usage of logical operators ($\vee/\wedge$), a resource tree (including the capability to represent redundancies of resources) can be created for each activity. This tree is similar to a fault tree. More information about fault tree analysis (FTA) can be found at [35, 56]

To clarify our mathematical approach we provide a short sample: We assume that there exists an activity Act_2. The set of attributes of this activity comprises two attributes. The first attribute A_1 represents the availability and the second attribute A_2 the integrity of the BPE. In order to perform this activity correctly, a resource R_1 "Server" (availability 80%, integrity 100%), a resource client PC R_2 (availability 100%) and, as can be seen in the figure, one of the two employees R_3, R_4 (availability 80%) are required. Using our formal model, this situation can be described as follows:

$$\begin{split} RR_2 = \{Act2; (R_1, A_1, 0.8, f_{1,1}(t), A_2, 1.0, f_{1,2}(t)) \wedge (R_2, A_1, 1.0, f_{2,1}(t)) \wedge \\ [(R_3, A_1, 0.8, f_{3,1}(t)) \vee (R_4, A_1, 0.8, f_{4,1}(t))]\} \end{split} \tag{6.3}$$

It is obvious that an alteration of a resource attribute's condition has an indirect influence on the corresponding activity itself. The impact of a threat on the attacked resource's attribute is defined in the threat's impact function itself ($\omega(t)$). In order to establish the link between the impact on the resource and the activity, we use function $f_{j,m}(t)$ which is independent of $\omega(t)$ but dependent on the resource's condition.

In the following subsection we provide further details on the formal description of threats, safeguards and their impacts.

6.2.2 A Formal Description of the Behavior and Effects of Threats and Safeguards

The formal representation of threats, their behavior and safeguards is a major prerequisite for our risk-aware simulations. Therefore, in this section we outline how threats and safeguards are formally described in our model in order to bridge the gap between business process management and security/risk management.

As our declared focus and central element is business process management, we decided that threats always affect attributes of business process elements such as the availability of a server or the execution time of a task.

The characteristics of a threat are dynamic in nature. Therefore, we decided to formally describe a threat through an impact function $\omega(t)$ which captures the characteristics of a threat such as behavior or speed.

We define $\mathcal{T} = \{T_1, \ldots, T_n\}$ as the set of all possible threats. Each threat T_i has the following parameters, which express impact of a threat on a business process element:

- p_n indicates the probability of occurrence in
- a given time interval $[t_0; t_1]$,
- the impact function $\omega_n(t)$ and
- the corresponding attribute A_n

To clarify the above-mentioned description, we provide the following simplified example: Let us assume a threat T_1 (e.g., malicious code) which has a negative effect on the attribute A_4 (e.g., availability or integrity), a rate of occurrence of p_1 (e.g., 70%) within the time interval 2 and 5.5 and the following impact function $\omega_1(t)$ (e.g. linear function or Weibull function). Then we can express this threat by the following equation:

$$[T_1; 0.7; [2, 5.5]; \omega_1(t); A_4]. \tag{6.4}$$

Threats can be prevented and mitigated by countermeasures (also commonly referred to as safeguards or controls). In our approach, countermeasures are grouped into three different categories (i.e. *preventive, blocking and reactive measures*) according to their behavior. The characteristics and distinguishing features of these categories are presented in the following paragraphs.

Preventive measures: This type of safeguards has a direct effect on a threat's occurrence probability. Examples of preventive measures against a fire-threat are the usage of fire-resistant materials in offices or the introduction of a non-smoking policy in a company. $\mathcal{PA} = \{PA_1, \ldots, PA_m\}$ is the set of all preventive measures. A specific preventive measure can be formally expressed by the following set of tuples:

$$PA_m := \{(T_k, \rho_k), \ldots\} \tag{6.5}$$

where T_k describes the corresponding threat and ρ_k the associated probability reduction. Thus, the probability of a threat p_n is reduced by ρ_n leading to the new occurrence probability $\tilde{p}_n = p_n - \rho_n$.

Blocking measures: Blocking measures are a special case of reactive measures. The specialty of this type of safeguard is that it immediately eliminates a threat upon its detection. Thus, threats eliminated by blocking measures will lead to no further consequences for business processes. A good example of a blocking measure is the filtering of emails. If the live-scan at an anti-virus scan center determines a dangerous mail, it immediately deletes or quarantines the mail.

In our model we define $\mathcal{BA} = \{BA_1, \ldots, BA_l\}$ as the set of blocking actions. Each blocking measure BA_l can be expressed as the following set of tuples:

$$BA_l := \{(T_k, \beta_k), \ldots\} \tag{6.6}$$

where T_k is the threat and β_k indicates the detection probability of the threat.

It is important to differentiate between the two probabilities $\tilde{p}_n$ and β_k. $\tilde{p}_n$ describes the occurrence probability of a threat while the probability β_k decides whether a threat is detected and immediately destroyed.

Reactive measures: A reactive measure can be defined as a safeguard that counteracts threats during an attack. An example of reactive measures is the manual removal of a malicious code .

In our model, reactive measures are composed of the succeeding three parts: (a) detection measures, (b) counter measures, and (c) recovery measures. The corresponding course of action is as follows: An active threat is the prerequisite for successful detection. According to the point of time of the detection respectively the threats behavior, an adequate counter measure (if existent) is invoked. The detection measure decides which counter measure will be invoked. The following example should highlight the reason behind this choice. Let us assume a fire-threat. If the fire is detected by a fire-detector, and a fire suppression system exists, the fire suppression system will be invoked. If the detection takes place by a pedestrian walking near the building, it is likely that the fire-brigade will be called in the first run.

Similar to detection, we assume that the recovery process is launched by the counter measure process. A slight difference between the relation of detection and countermeasure and countermeasure and recovery measure is that countermeasures and recovery measures can overlap. In other words, the countermeasure directly starts if detection is over, the recovery can start while the countermeasure is still active.

In a simplified manner the phases can be summarized as follows: Detection $\rightarrow$ Counter Measures $\rightarrow$ Recovery.

Furthermore, we make the following assumptions: The detection measure does not influence the threat itself in any way. The detection is active in every time step and the predefined detection period starts as soon as there is a recognizable change in the attribute's condition function.

We define a detection measure as:

$$DM_k := \{T_j, A_i, dm_k(t), (CM_m, \ldots)\} \tag{6.7}$$

where T_j represents the threat, which can be detected by a specific detection measure DM_k. A_i represents the corresponding attribute and $dm_k(t)$ is the function that provides information about the probability of detecting the threat T_j at a given "attribute's condition". The counter measures are expressed by CM_m, which can be a multidimensional vector. The usage of the function dm_k enables us to define a threat that has to be detected once the damage is x$\%$. An example would be a burning house. It is very unlikely that nobody recognizes that the house is exposed to fire-threat when half of the house is already destroyed.

The counter measures have a direct influence on a threat's state and therefore affect the impact function $\omega_n(t)$ of the corresponding threat T_n.

A specific counter measure CM_m is expressed as:

$$CM_m := \{cm_m(t), (RM_n, \ldots), (tc_n, \ldots)\} \tag{6.8}$$

where $cm_m(t)$ is the function describing the influence on the threat's impact function, RM_n are the required recovery measures and tc_n is the threshold holding information about the starting point of the recovery.

The influence on the threat's impact can be expressed by the new impact function:

$$\tilde{\omega}_n(t) := \omega_n(t) \cdot (1 - cm_m(t)) \tag{6.9}$$

In order to determine the starting point t_r of the recovery measure RM_n, we set up the following assumptions:

1. $\tilde{\omega}_n(t_r) = tc_n$
2. $\tilde{\omega}'_n(t_k) \leq 0$

The counter measure is stopped once $\tilde{\omega}_n(t) = 0$.

The recovery measure has a direct influence on the attribute's condition function $z_i(t)$. It is further specified through a recovery function $rm_i(t)$. The influence on the condition of an attribute can be seen as a new condition function:

$$\tilde{z}_i(t) := z_i(t) + rm_i(t) \tag{6.10}$$

The recovery ends once the condition is $\tilde{z}_i(t) = 1$.

In order to clarify our formal model we demonstrate in the following how our approach can be applied to model an activity's attributes "availability" and "integrity".

6.2.3 Modeling the Activity's Attribute Availability

For simulation purposes we assume that an activity possesses an attribute "degree of completion" $G : \mathbb{R} \to [0, 1]$ (continuous). Further, the activity is considered completed once $G = 1$.

Finite activities have the following characteristics:

$$\exists \quad \tilde{t} \in \mathbb{R} \text{ with } G(\tilde{t}) = 1 \tag{6.11}$$

$$\exists \quad g, \text{ integrable, with } G(t) = \int_0^t g(u)du \tag{6.12}$$

For this reason, the execution time of a process activity can be derived by solving the following integral equation:

$$G(\tilde{t}) = \int_0^{\tilde{t}} g(u)du \tag{6.13}$$

In order to determine the impact of a threat attacking the availability attribute of an activity, function (6.13) has to be extended with the threat's impact function $\omega(t)$:

$$G(\tilde{t}) = \int_0^{\tilde{t}} g(u) - \omega(u) du \tag{6.14}$$

6.2.4 Modeling the Activity's Attribute Integrity

Some activities require the attribute "integrity". The measurement of a loss of integrity is similar as described in the previous subsection 6.2.3. We assume the integrity of a certain activity to be a real function $i : \mathbb{R} \rightarrow [0, 1]$. As long as no threat is active, we set $i(t) = 1$.

The loss of integrity can be formally described as follows:

$$IL(t) = \int_{t_0}^{t} (1 - i(u)) du \tag{6.15}$$

While no threat endangers the integrity attribute, the "loss of integrity" is constantly equal to 0, $IL(t) = 0$. In order to consider the impact of a threat on the activities' integrity attribute, we extend the function (6.15) with the threat's impact function $\omega(u)$:

$$IL(t) = \int_{t_0}^{t} (1 - (i(u) - \omega(u))) du \tag{6.16}$$

with $\omega(u)$ being the impact of a threat on the integrity attribute and t_0 being the starting time of the activity. The enhanced function makes it possible to measure the resulting loss of integrity.

6.2.5 Relation between Resources' and Activities' Attributes

Activities depend on the functionality of their resources. Thus, impacts can have an indirect influence on the corresponding activity's attribute. In our model, we assume that this interrelation is proportional to the difference emerging from the actual resource's attribute condition and the needed attribute condition. The needed state of an attribute ν can be obtained from the corresponding resource requirements (see section 6.2.1, equation (6.3)).

Let N_{t_m} be the current condition of a resource's attribute $A_i(t)$ at the point in time t_m, $0 < N_{t_m} < 1$. If the condition N_{t_m} reaches the threshold ν, then the condition's alteration has an influence on the linked activity's attribute. To realize this, we define the following support function:

$$\varphi(t) = f(\nu - N_t) \tag{6.17}$$

$$f(0) = 0 \tag{6.18}$$

The support function $\varphi(t)$ can be understood as function of threat impact on the activity's attribute, which depends only on the resource's condition and is independent of the original threat's impact function.

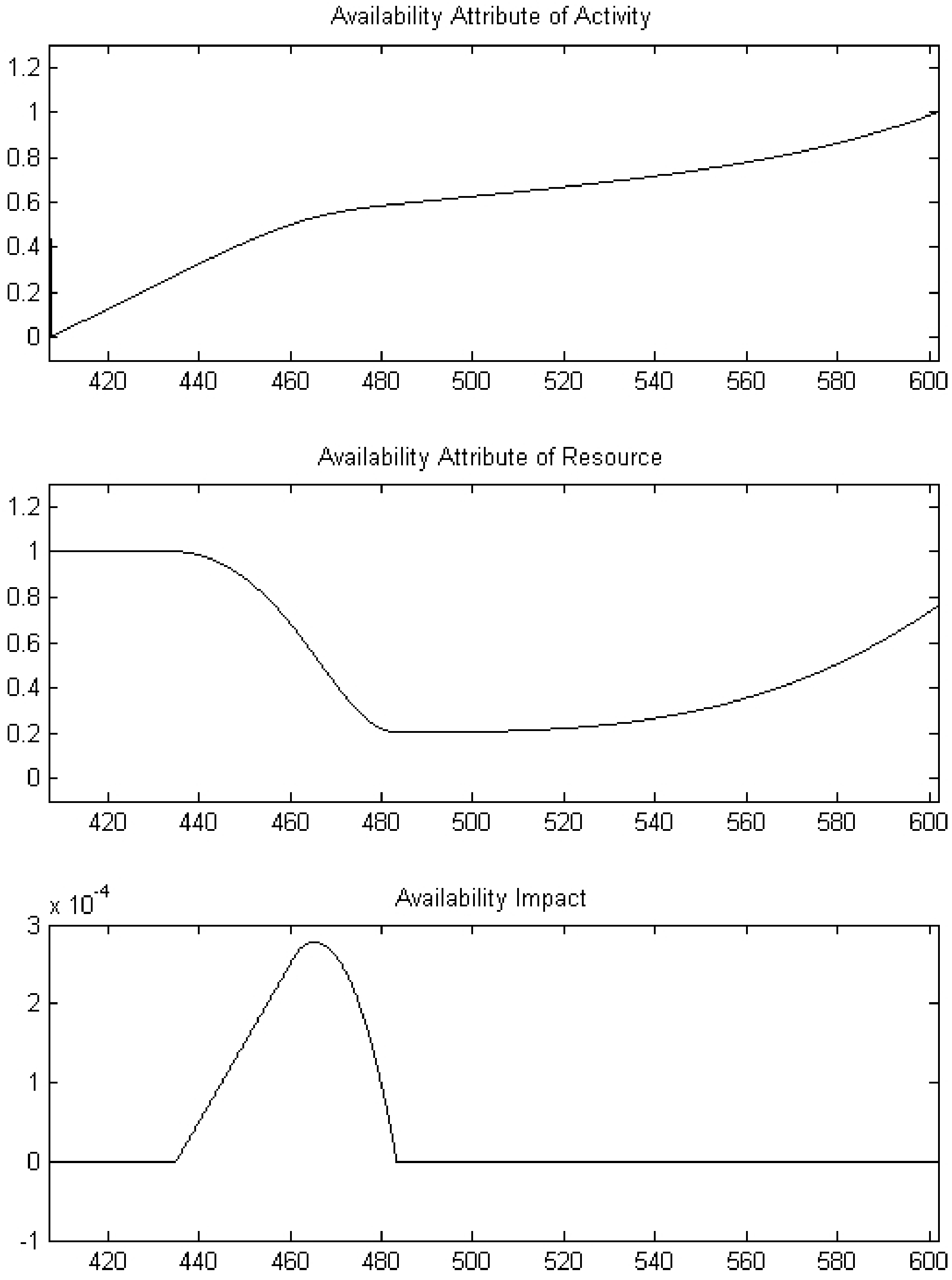


Figure 6.4: Influence of a Threat and its Consequences on the Availability Condition Function. In Ascending Order: Impact Function, Resource Attribute Condition and Activity Attribute Condition

Fig. 6.4 illustrates the influence of a threat impact on the linked resource’s availability condition. Additionally, it shows that an attacked resource’s availability has an indirect influence on the activity’s completion function. The lower chart depicts the threat’s impact over time, while the middle chart shows the according impact of the threat on the availability of the affected resource over time. The upper chart shows the resulting impact on the continuous completion function of the assigned activity (leading to an increase in the execution time). In this section, we outlined how relations between activity attributes and resource attributes can be described using the example of the attribute "availability". This example applies analogously to all similar cases (e.g., integrity attribute).

6.3 Formal Description of Resource Re-Allocation Elements

In this section we introduce our concept of resource re-allocations. A resource allocation can be generally seen as a workaround or a way to improve the utilization of a resource. In our approach, the trigger for re-allocations are changes in the process-, activity- or resource attribute's condition. We define three archetype sets for resources, activities and processes. Each set contains one or more indicators and one or more subsets of possible resources for a successful allocation.

$$RAl(R_i) := \{(\underbrace{A_j, \leq / \geq W_{i,j}, [t_n, t_m]}_{indicator\ sequence}, PR_{i,j}), \ldots\} \tag{6.19}$$

$$RAl(Act_k) := \{(\underbrace{A_l, \leq / \geq V_{k,l}, [t_n, t_m]}_{indicator\ sequence}, \bigcup_{i,j} PR_{i,j} : \forall R_i \in AsR_k), \ldots\} \tag{6.20}$$

$$RAl(process_g) := \{(\underbrace{A_h, \leq / \geq U_{g,h}, [t_n, t_m]}_{indicator\ sequence}), \ldots\} \tag{6.21}$$

where in equation (6.19) $R_i \in \mathcal{R}$ is the certain resource, A_j one of its attributes. $W_{i,j}$ is the threshold for the attribute's A_j condition ($z(A_j)$) which is directly obtained from the corresponding resource requirements RR_n. Therefore $W_{i,j} \widehat{=} Z_k$, where Z_k is the threshold from resource R_i and attribute A_j from the corresponding $RR_{n|R_i \in AsR_n}$. The relational operators $\leq$ / $\geq$ determine if the threshold has to be undershot / overshot for a successful impact of a threat. $[t_n, t_m]$ is the time interval in which the threshold is valid. $PR_{i,j}$ is a set of possible resources that are able to successfully proceed the original resource's (R_i) task. The elements of $PR_{i,j}$ are tuples of the form: (R_m, p_m), where R_m is the resource that could replace the original resource and p_m the corresponding percentage to which the resource's attribute is needed for the specific activity. It is possible to combine two or more such tuples with the logical operator $\wedge$.

In equation (6.20), Act_k is the specific activity, A_l one of its attributes, $V_{k,l}$ the threshold for the attribute's condition as described above. To get all possible allocation resources for an activity, we unite every $PR_{i,j}$ of the activity's resources. In equation (6.21), $process_g$ is a certain process,

A_h one of its attributes, $U_{g,h}$ the threshold for the attribute's condition. We assume that an affected process has to have an affected activity as well. Therefore it has only the indicator sequence and no set of possible resources for each attribute.

6.4 Formal Description of Activity Re-Allocation Elements

In order to diminish the impacts of an incident, it is sometimes necessary to substitute an affected activity for another activity or a subprocess. Therefore, although it is not the main focus of this thesis, we briefly want to discuss the concept of activity re-allocation in this section. The approach is strongly aligned to our resource re-allocation concept.

In the following, we briefly provide an example to clarify the need for activity re-allocations: Let us assume an activity that is heavily supported by information systems, such as the automated control of a SCADA system. If the information system has a malfunction or is not available it might be necessary to manually control the system. This could be represented by an activity re-allocation.

As mentioned above, the approach is based on the concept of resource re-allocations in the previous sections. Therefore, the indicator sequence is built in the same way as in the formulas (6.19)(6.20)(6.21). The difference to resource allocation is that the set of possible substitutes $PAl_{k,l}$ contains activities and/or subprocesses instead of resources.

$$AAl(Act_k) := \{(\underbrace{A_l, \leq / \geq Z_{k,l}, [t_n, t_m]}_{indicator\ sequence}, PAl_{k,l}), \ldots\} \tag{6.22}$$

$$\text{with } PAl_{k,l} := \{pal_1, \ldots, pal_n\}, n \in \mathbb{N}$$

$$\text{and } pal := \begin{cases} Act_k \in \mathcal{A}ct \\ process_l \in \mathcal{P} \end{cases}$$

$$\begin{aligned} AAl(process_g) := \{(&\underbrace{A_h, \leq / \geq K_{g,h}, [t_n, t_m]}_{indicator\ sequence}, \\ &\bigcup_{k,l} PAl_{k,l} : \forall Act_k \in AsAct_g), \ldots\} \end{aligned} \tag{6.23}$$

6.5 Sample Scenario

In this section we present a simplified sample scenario. This scenario pursues the aim to outline how our formal model can be applied. We deliberately decided on an simplified scenario where the complexity level is manageable. However, the approach is also capable to manage complex structures and scenarios if required.

The sample process (telephone support service) is performed in a call center of a fictive company called ACME. The process follows a frequently used multi-level structure: The first level (Activity 1) support is responsible for initially answering all incoming calls. If the first level support can not resolve the request of the customer, the call will be forwarded to the next stage (second level support or Activity 2). Similar to the first level support activity, requests that cannot be remediated by the second level support are escalated to third level support (Activity 3).

In order to initially plan the resources and demonstrate the capability of resource re-allocations we introduce the following assumptions: Historical data of the organization provide the information that under normal conditions, approximately 2/3 of the calls can be handled by the first level support and only 1/3 of the calls are forwarded to the next level. Further, the second level support can directly resolve half of the forwarded issues.

The prerequisite for the execution of Activity 1 is a person with skill level A. In our case, three persons (with the corresponding skill level A) are assigned to Activity 1. For the higher support levels, we assume that a skill level of B is required for second level support and skill level of C is required to perform tasks in the third level support.

Due to cross-skill trainings in the company, we further assume that employees with skill level B can replace employees with skill level A and persons with skill level C are able to act as deputy for persons with skill level B.

For reasons of clarity, we schematically outlined the whole scenario in Figure 6.5.

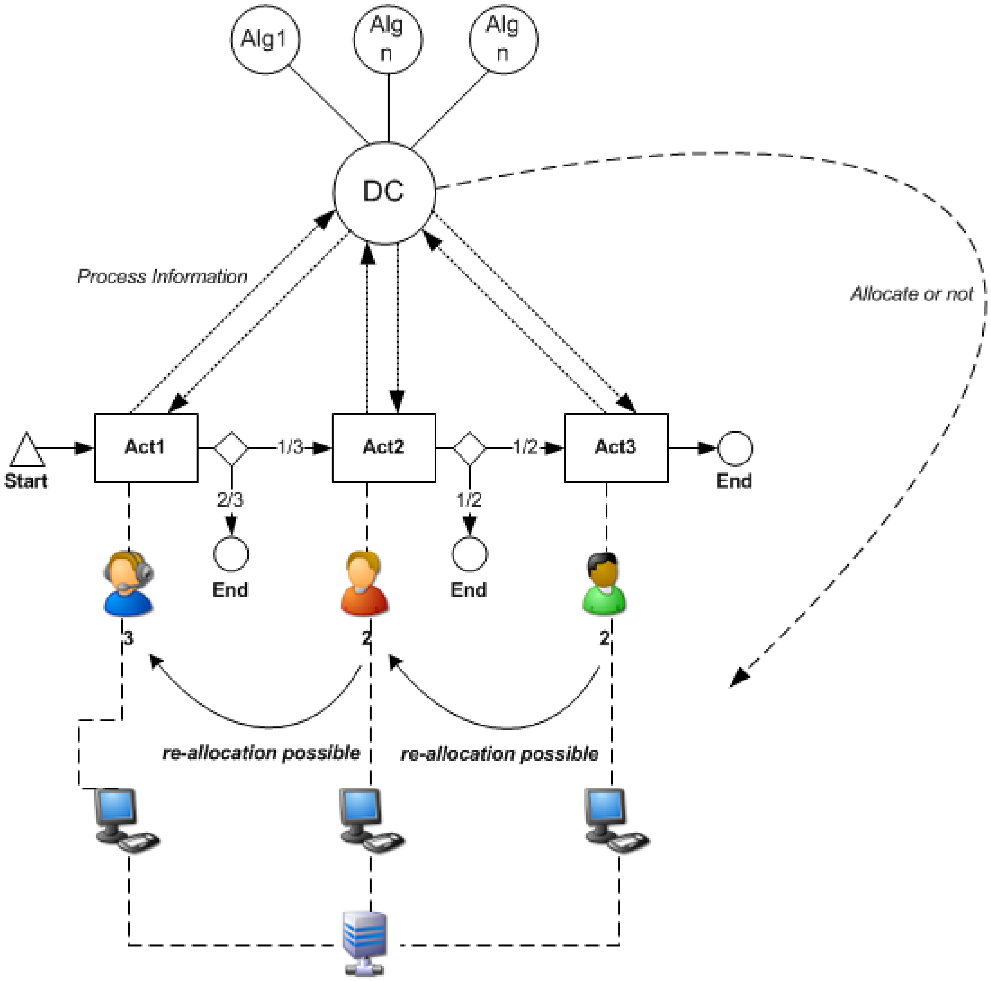


Figure 6.5: Decision Component

6.6 Formal Description of the Sample Scenario

In this section, we present a simplified sample scenario to clarify our approach. The sample scenario is schematically outlined in Section 6.5. The scenario can be described as follows with our formal model:

$$(A_1 \mathrel{\widehat{=}} availability,\ A_2 \mathrel{\widehat{=}} backlog,\ A_3 \mathrel{\widehat{=}} proceeds)$$

$$
\begin{aligned}
AsR_1 &:= \{R_1, R_2, R_3\} \\
AsR_2 &:= \{R_4, R_5\} \\
AsR_3 &:= \{R_6, R_7\} \\
AsAct_1 &:= \{Act_1, Act_2, Act_3\} \\
RR_1 &:= \{Act_1; \{\underbrace{(R_1, A_1, 70\%, f_{1,1}(t))}_{q_1}, \ldots \\
&\quad \underbrace{(R_2, A_1, 70\%, f_{2,1}(t))}_{q_2}, \underbrace{(R_3, A_1, 70\%, f_{3,1}(t))}_{q_3}\}\} \\
RR_2 &:= \{Act_2; \{\underbrace{(R_4, A_1, 80\%, f_{4,1}(t))}_{q_4}, \ldots \\
&\quad \underbrace{(R_5, A_1, 80\%, f_{5,1}(t))}_{q_5}\}\} \\
RR_3 &:= \{Act_3; \{\underbrace{(R_6, A_1, 80\%, f_{6,1}(t))}_{q_6}, \ldots \\
&\quad \underbrace{(R_7, A_1, 80\%, f_{7,1}(t))}_{q_7}\}\} \\
As(Act_1) &:= q_1 \vee q_2 \vee q_3 \\
As(Act_2) &:= q_4 \vee q_5 \\
As(Act_3) &:= q_6 \vee q_7 \\
RAl(R_1) &:= \{(A_1, \leq, \overbrace{W_{1,1}}^{=70\%}, [t_0, t_{end}], PR_{1,1})\}
\end{aligned}
$$

$$\begin{aligned}
PR_{1,1} &:= \{(R_4, 100\%), (R_5, 100\%)\} \\
RAl(R_2) &:= \{(A_1, \leq, 70\%, [t_0, t_{end}], PR_{2,1})\} \\
PR_{2,1} &:= \{(R_4, 100\%), (R_5, 100\%)\} \\
&\vdots \\
RAl(R_5) &:= \{(A_1, \leq, \overbrace{W_{5,1}}^{=80\%}, [t_0, t_{end}], PR_{5,1})\} \\
PR_{2,1} &:= \{(R_6, 100\%), (7_5, 100\%)\} \\
&\vdots \\
RAl(R_7) &:= \{(A_1, \leq, 80\%, [t_0, t_{end}], \emptyset)\} \\
RAl(Act_1) &:= \{(A_2, \geq, \underbrace{V_{1,2}}_{=5}, [t_0, t_{end}], PR_{1,1} \cup PR_{2,1} \cup PR_{3,1})\} \\
&\vdots \\
RAl(Act_3) &:= \{(A_2, \geq, \overbrace{V_{3,2}}^{=2}, [t_0, t_{end}], PR_{6,1} \cup PR_{7,1})\} \\
RAl(process_1) &:= \{(A_3, \geq, \underbrace{U_{1,1}}_{50}, [t_0, t_{end}])\}
\end{aligned}$$

6.7 Chapter Summary

In this section, we first introduced our general approach for risk aware business process management. We highlighted how we intend to diminish the gap between business process management and security-related respectively business continuity related approaches. In the further course of this chapter, we presented the steps which were necessary to conduct sustainable risk-aware business process management. After presenting the conceptual model and the methodological approach we outlined our formal model.

In this formal model, we showed how our approach extends typical business process elements. We further outlined our threat model and its essential parts in order to represent the behavior of incidents (i.e. interaction between threat and safeguard aspects) and to determine the impact on business processes.

Thereafter, we presented our re-allocation approach. In a nutshell the objective of formally expressing re-allocations of activities and processes is to model workarounds. The mathematical description serves as a basis for the Simulink prototype which is presented in the next chapter.

In Section 6.5 of this chapter, we provided a sample scenario in order to illustrate our approach and its applicability for resource re-allocations.

The Prototype

> “ The superior man is modest in his speech, but exceeds in his actions.
>
> CONFUCIUS

In order to test and evaluate our approach and formal model we used a prototype implemented in Simulink®. The reasons behind our decision to implement our proof-of-concept in Simulink® were the flexibility and built-in simulation support.

In the following sections, we further clarify the implementation of our formal model enabling resource allocation and demonstrate how we simulate resource allocation using Simulink®.

7.1 Re-Allocation Algorithm

In this section, we outline our currently used re-allocation algorithm. Figure 6.5 demonstrates how our resource (/activity) re-allocation decision component works. In every simulation step, the attribute information of processes, activities and resources is evaluated against the previously introduced re-allocation rules.

If the condition of a rule is true (e.g. attribute below a certain threshold) and the re-allocation is possible, the re-allocation will be performed. The modular design of the resource allocation block creates the possibility to easily change the allocation algorithm.

Previously, we declared the necessary sets and indicators for a resource re-allocation in the context of business process management. To understand how we use those sets of possible resources and indicators, we present the algorithm that was implemented in the toolkit Simulink®:

Table 7.1: Pseudo Code: Resource Re-Allocation Algorithm

```
For each process attribute ($\forall A_h \in RAl(process_g)$)
 If indicator sequence is true
 ($z(A_h) \leq / \geq U_{g,h}$ in interval $[t_n, t_m]$)
   For each process activity attribute
   ($\forall A_l \in RAl(Act_k) | Act_k \in AsAct_g$)
     If indicator sequence is true
     ($z(A_l) \leq / \geq V_{k,l}$ in interval $[t_n, t_m]$)
       For each process activity resource attribute
       ($\forall A_j \in RAl(R_i) | R_i \in AsR_k$)
         If indicator sequence is true
         ($z(A_j) \leq / \geq W_{i,j}$ in interval $[t_n, t_m]$)
           Choose a resource from the
           set of possible resources for $R_i$
           ($R_i \in PR_{i,j}$)
```

```
        Else
          Choose a resource from the
          set of possible resources for $Act_k$
          ($R_i \in \bigcup_{i,j} PR_{i,j}$)
        Assign resource $R_i$ to activity $Act_k$
```

As mentioned before in some cases a sole resource re-allocation is insufficient to reduce the negative effects of a threat on a process or activity. Therefore we also introduced the possibility of an activity allocation which works in an analogous way:

Table 7.2: Pseudo Code: Activity Re-Allocation Algorithm

```
For each process attribute ($\forall A_h \in AAl(process_g)$)
  If indicator sequence is true
  ($z(A_h) \wedge / \vee K_{g,h}$ in interval $[t_n, t_m]$)
    For each process activity attribute
    ($\forall A_l \in AAl(Act_k) | Act_k \in AsAct_g$)
      If indicator sequence is true
      ($z(A_l) \leq / \geq Z_{k,l}$ in interval $[t_n, t_m]$)
        Choose a subprocess from the
        set of possible substitutes for $Act_k$
        ($pal_n \in PAl_{k,l}$)
      Else
        Choose a subprocess from the
        set of possible substitutes for $process_g$
        ($pal_n \in \bigcup_{k,l} PAl_{k,l}$)
      Assign subprocess $pal_n$ to process $process_g$
```

7.2 Simulink Proof-of-Concept-Prototype

This section describes how our proof-of-concept-prototype is implemented. We used the sample scenario presented in Section 6.5.

Figure 7.1 illustrates the main layer of our Simulink® implementation. It represents one business process and the corresponding business process elements.

The process consists of three activities which are represented by the subsystems *Activity 1, Activity 2, Activity 3*. In order to model the flow (i.e. escalation to second level support or third level support), two decisions *Decision1, Decision2* are introduced. Further, each activity requires resources which are represented by resource management subsystems *RM1, RM2, RM3* and one server resource block for all activities (Servers). Within the resource management subsystem we realized the assigned PCs. Figure 7.2 illustrates how we implemented the resource management subsystems.

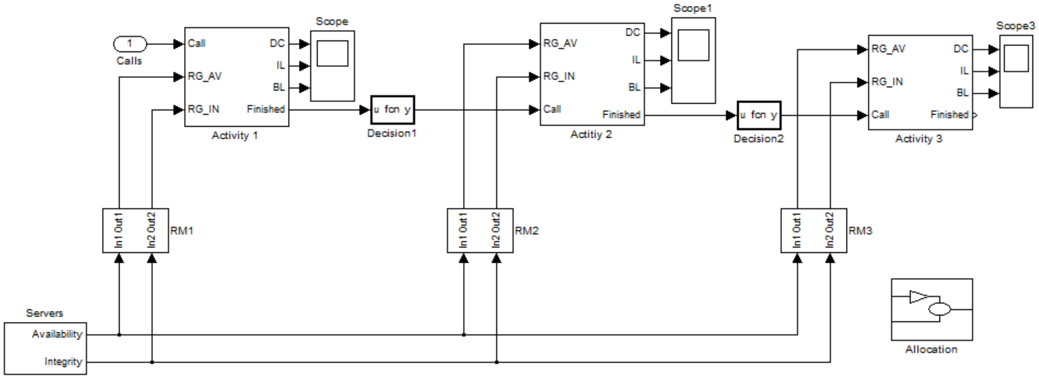


Figure 7.1: Simulation Model: **Main Layer**

Additionally in the **main layer**, we find the allocation subsystem (*Allocation*) which will be described later on in this section.

For the illustration of our process, we assume one financial attribute which is *proceeds*. Further we assume that our activities have two attributes which are *degree of completion (DC)* and *integrity* *loss (IL)*. The degree of completion attribute depends on the availability attribute of the needed resources whereas the integrity loss attribute depends on the corresponding resources integrity attribute. As our sample case should only deliver a demonstrative example, we consider the integrity attribute only for the server.

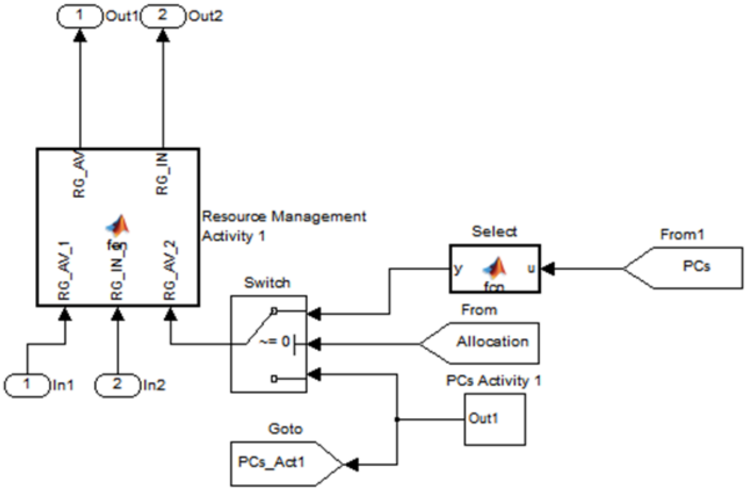


Figure 7.2: Resource Management Subsystem of Activity 1

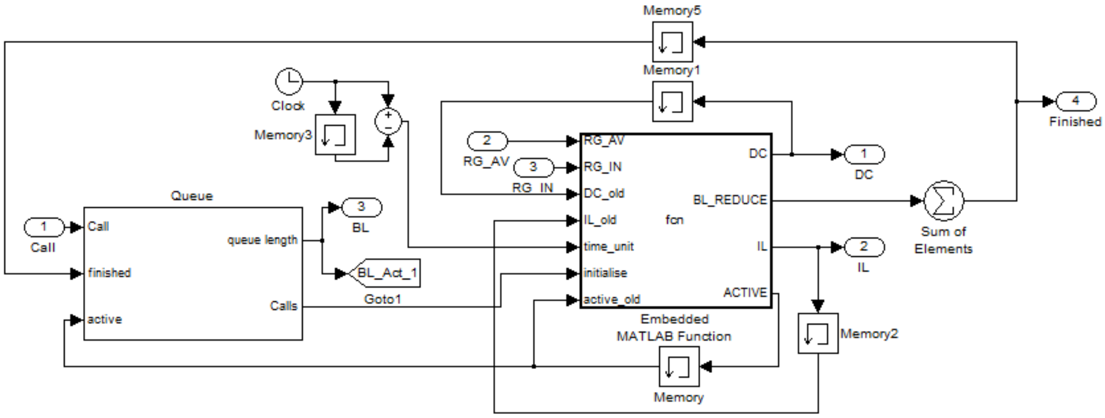


Figure 7.3: Simulation Model: **Activity Layer**

Figure 7.3 highlights the structure of an activity layer. The activity subsystem has the following input signals:

- the assured resources (*RG_AV, RG_IN*)
- the degree of completion and integrity loss attribute (*DC_old, IL_old*) of the previous time step
- the help signal *time_unit* which is used to determine the length of the actual time step. This is necessary to determine the integration intervals.
- the initialize signal from the Queue block. This Boolean signal regulates when an activity (or one of its instances) is started.
- the input signal *active_old* captures information on the state of the activity in the previous time step (i.e. if the activity was active or not)

The main component of the subsystem is an *Embedded MATLAB Function* which simulates the activity. Firstly, the difference between required and assured ((*RG_AV, RG_IN*)) resources is determined in order to get the actual completion speed and the integrity mismatch, respectively. The next step is the calculation of the degree of completion and integrity loss attribute. Finally, it is determined if an instance finished its execution and how many instances are active. The input signal *active_old* gets updated at every time step and acts as the output signal *ACTIVE* which is required by the *Queue* block. The backlog reduce signal *BL_REDUCE* indicates if an instance has finished a task in the actual time step.

The *Queue* block on the left handles the incoming calls. It contains the input signals *Call, finished* and *active*. The block calculates the value of the queue length (*queue length*) for the corresponding activity and the initialize indicator (*Calls*) for the main block *Embedded MATLAB function*. Whenever an incoming call appears (*Call=1*), the length of the queue is increased by 1. Whenever an instance finishes a task (*finished=1*), the queue is decreased by 1. The *active* signal gives information about the amount of active or nonactive instances, to decide whether a call gets forwarded to the Embedded MATLAB Function block.

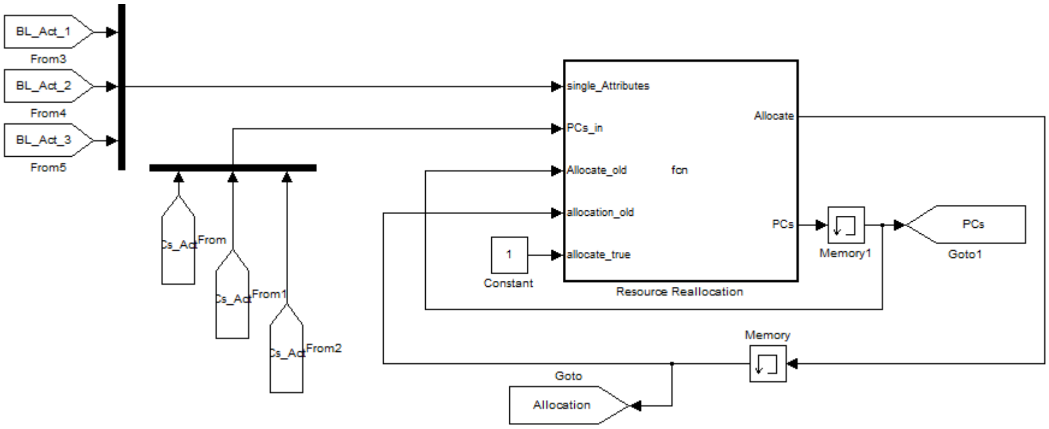


Figure 7.4: Simulation Model: **Allocation Layer**

Figure 7.4 depicts the **allocation layer**. It is a subsystem of the main layer. It has one main block realized as an embedded Matlab function (*Resource Reallocation*). This block has the following input signals:

- *single_Attributes*: represents the backlog of the activities *BL_Act_1, BL_Act_2, BL_Act_3*. The sum of these values is used to calculate the aggregated backlog.
- *PCs_in*: this signal contains information about the availability attribute of the PCs.
- *Allocate_old*: this Boolean signal provides information about previous re-allocations.
- *Allocation_old*: whenever a re-allocation takes place, the signal is set true.
- *Allocate_true*: help signal to activate/de-activate re-allocation.

On the basis of our formal model and the above described input signals, the embedded Matlab function determines if and how an allocation is needed. It has the output signals Allocate which is the update signal of *allocation_old*. PCs is the actual permutation of the PCs.

7.3 Results and Discussion

This section discusses the results gained by our simulation of the sample scenario. We compare two different settings: (1) no re-allocation considered; (2) resource allocation available.

In the first scenario (Figure 7.5), the threat attacks an instance of activity 1 close to time step 400. Thus, the instance cannot proceed its intended task. The result of this inability to perform the activity is an immense increase of the backlog of activity 1(c).

The remaining instances are not able to compensate the outage or to reduce the backlog. Therefore, the backlog steadily increases until the recovery of the attacked instance. In our scenario, approximately around time step 980 the instance works normal again. It is apparent that the instance is in an operational state before (approximately at time step 730), but in an inefficient way. The obvious lesser completion rate of activity 1 results in an almost stagnancy of the financial attribute proceeds of the process. As no threat affects the execution of activities 2 and 3, there is no increase of their backlogs.

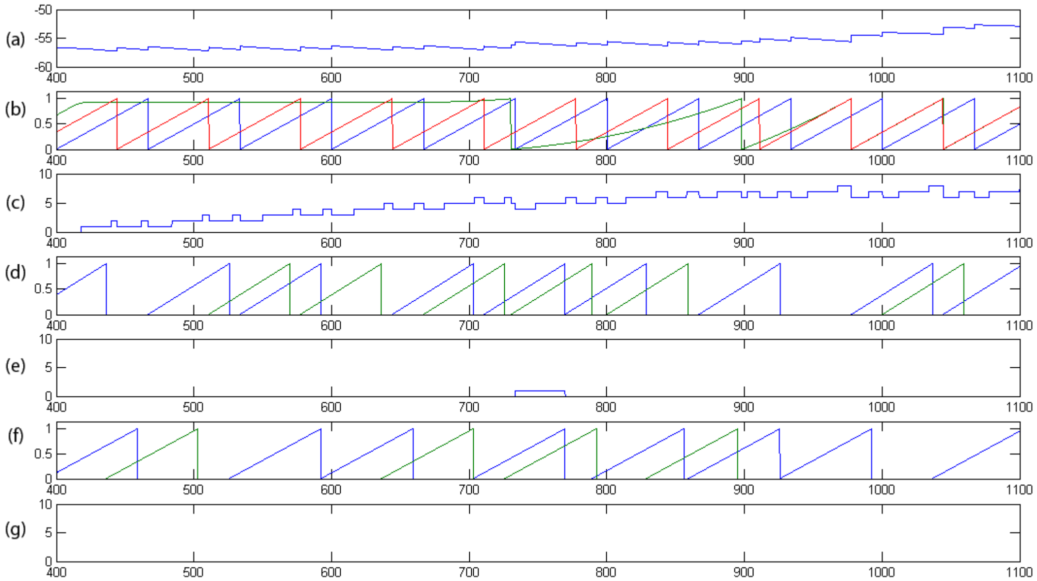


Figure 7.5: Scenario: No Resource Allocation

In the second scenario (Figure 7.6), one can see the simulation results for a business process with enabled resource re-allocation. In subplot (a), the financial attribute proceeds (process level) is depicted. The subplots (b), (d) and (f) show the degree of completion of the activity instances.

Activity 1 (b) has three instances, activity 2 and 3 (d)(f) have two instances. The subplots (c),(e) and (g) highlight the corresponding backlogs for each activity. For the sake of readability, we chose to limit the display area to the relevant time frame of the simulation (i.e. from time step 400 to 1100).

As in the previous scenario, we simulated a threat that attacks an instance of activity 1 (b) time step 400. This attack results in the idleness of its degree of completion. Therefore the backlog of activity 1 (c) increases like in the before-mentioned scenario. As soon as the caused backlog reaches our pre-defined threshold (=5), a resource from activity 2 (d) gets re-allocated to activity 1. This happens at time step 510.

The resource remains at activity 1 until it gets called back to its assigned activity due to the increase of activity 2's backlog (e) to the defined threshold. After the backlog of activity 2 is reduced to an acceptable level, the same instance is re-allocated again to activity 1. As it is not possible for a single instance of activity 2 to decrease the backlog appropriately, an instance from activity 3 (f) gets allocated to activity 2 around time step 750. This results in an increase of activity 3's backlog (g) and in a decrease of activity 2's backlog. The original instance of activity 1 is fully recovered around time step 980. The allocated resources are transferred back to their original assigned activities in order to reduce the emerged backlogs.

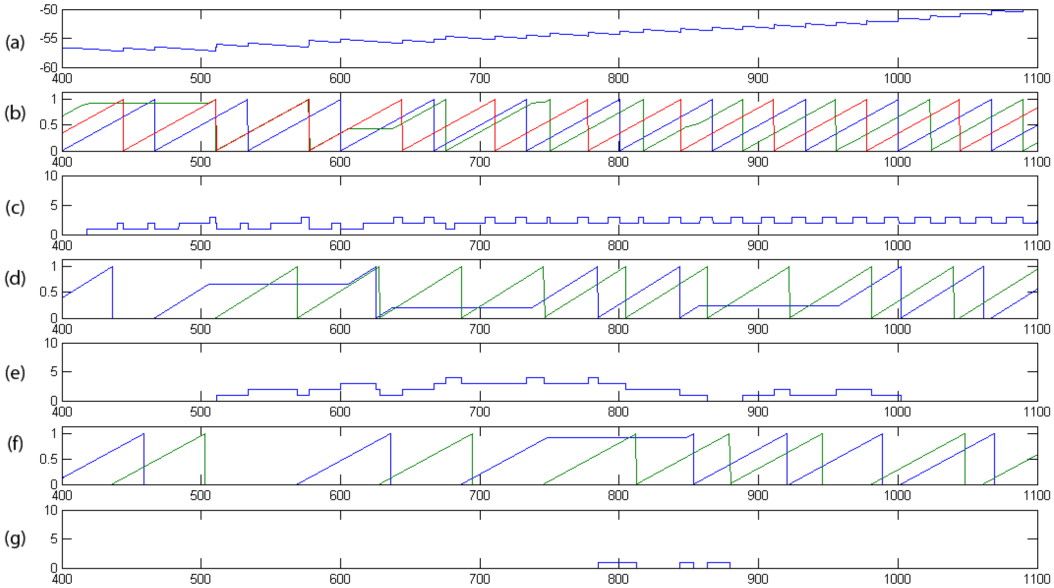


Figure 7.6: Scenario: Resource Allocation

When comparing the presented scenarios, we can observe that in the second scenario the impact on the process attribute proceeds is very low due to the effective and efficient resource allocation. Contrary to what we have observed in the second scenario, one can see in the first scenario that the threat on activity 1 results in major impacts on the process attribute proceeds as there is a major downtime in the completion rate of activity 1.

7.4 Chapter Summary

Based on the results of the previous chapters, we introduced the Simulink-prototype which was used to test our formal approach on dynamic resource allocations. At the beginning of the chapter, we outlined how we realized the re-allocation algorithms for activities and resources and later on described the architecture and main layers of the prototype.

Finally, we discussed the gained results for the sample scenario case which was described in Section 6.5. We demonstrated that the representation of workarounds, such as replacing an employee with another, can be outlined by our approach.

Part III
The Meta model

Open Models

> “Things should be made as simple as possible, but not any simpler.
>
> ALBERT EINSTEIN

The Open Model Initiative (OMI) has the objective to establish a community that “ ... deals with the creation, maintenance, modification, distribution, and analysis of models”[71]. The platform provided by the initiative enables the creation and use of a variety of models and is not limited to any concrete research area. The model presented in this thesis is available as a project in the information security community of the Open Model Initiative [100].

8.1 Extended Business Process Elements

In this section, we provide details about the basic elements of our process language. The components used are mainly derived from the business process model described in [67, p. 13]. Some components have been slightly adapted in order to suit our needs. Figure 8.1 schematically outlines the relations between the modeling entities.

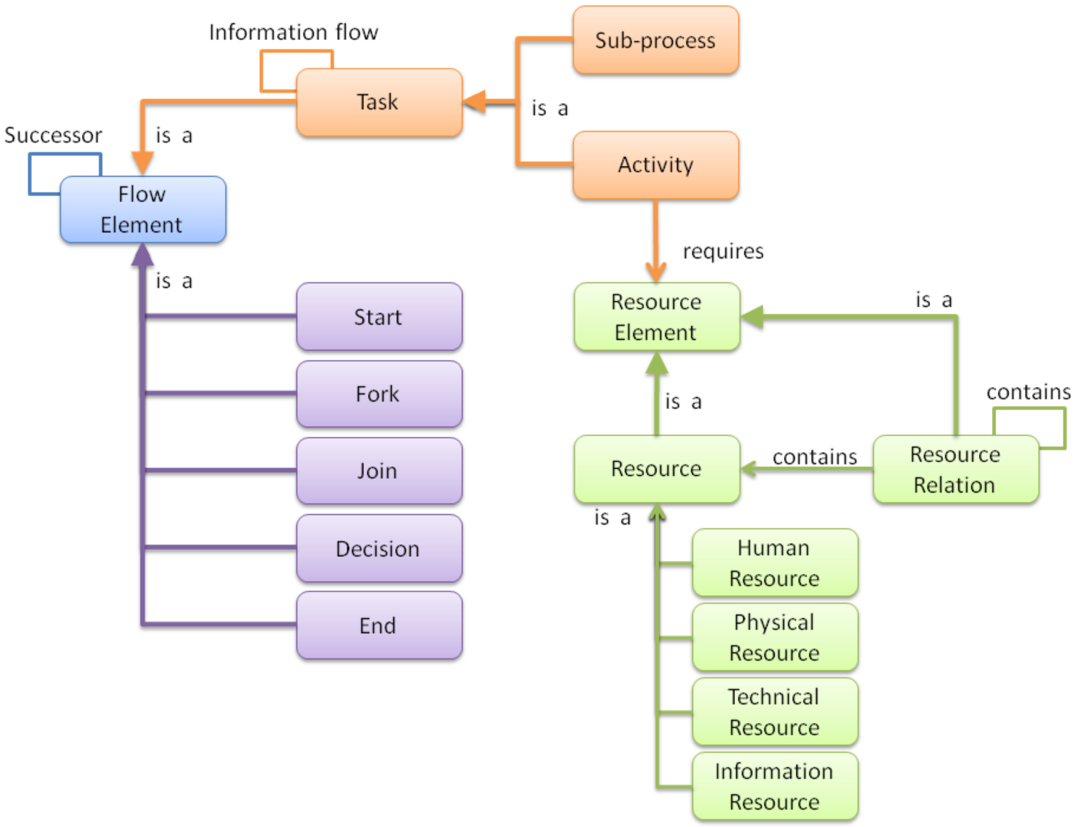


Figure 8.1: Business process model derived from [67, p. 13]

Process: The process element contains all essential information on an abstract level. This component is mainly used later on in adapted process maps which outline the dependencies both, under normal and emergency conditions.

Table 8.1: Attributes of a process element within the meta-model

Name	Type	M/C	Description
ID	Integer	M	a unique identifier in order to enable simulation operations and analyzing steps
NAME	String	M	a readable name for the process. It is recommended to keep this name unique.
FINANCIAL VALUE	Enumeration	C	a qualitative description (i.e. negligible, low, medium, high, very high) of the financial value of the process
STRATEGIC VALUE	Enumeration	C	a qualitative description (i.e. negligible, low, medium, high, very high) of the strategic value of the process
SPECIAL TIME PERIODS	Table	C	this table specifies peak periods within the process (e.g. summer season, Christmas trading)
INTERRUPTIBLE	Enumeration	C	this gives important information whether preemptive or non-preemptive approaches should be used scheduling. The default option is set to yes.
CUSTOMER INTERFACE	Enumeration	C	This attribute provides information whether the process has a direct interface to the customer. This is important as activities that have a high customer visibility are more likely to cause negative impacts on brand and reputation. Default is set to “No”. Other options comprise key accounts, accounts or shareholder/partner.

KEY CUSTOMERS	Longstring	C	this attribute describes the customers that are targeted by the process. As business continuity responses may vary corresponding to the customer group, this information can improve the response planning.
KEY INFORMATION	Longstring	C	describes the key information assets
KEY APPLICATIONS	Longstring	C	this attribute provides information in a verbose form about key applications used in the process. This information is essential for a first high-level analysis and for specifying the scope for further analysis steps.
KEY SUPPLIER	Longstring	C	this attribute provides details about essential supplier. For a comprehensive integration of supply risk aspects and service level analysis, we kindly refer to [59]
RTO	Time	C	According to the German Federal Office for Information Security the“... recovery time objective (RTO) specifies the time in which the process is intended to be recovered.”[12, p. 45]. In our model, this time-period is relevant for analyzing whether the process can be finished within the required time-frame.
MTPD	Time	C	The maximum tolerable period of disruption defines the time span during which a process can be interrupted or unavailable before the company becomes damaged irreversibly. [16, p.13]
CONFIDENTIALITY THRESHOLD	Float	M	A float number between 0 and 1 indicating the level of confidentiality that has to be guaranteed.

INTEGRITY THRESHOLD	Float	M	A float number between 0 and 1 indicating the level of integrity that has to be guaranteed.
AVAILABILITY THRESHOLD	Float	M	A float number between 0 and 1 indicating the level of availability that has to be guaranteed.
CONFIDENTIALITY	Float	M	current level of confidentiality
INTEGRITY	Float	M	current level of integrity
AVAILABILITY	Float	M	current level of availability
PROCESS OWNER	Interref	C	reference to an employee of the resource model
COMMENT	String	C	A comment for verbal description of the process.

8.1.1 Flow elements

The flow elements have been mainly derived from the ADOxx Default Library. Therefore, in the following only a short description of the different flow elements is outlined.

Start: The start element has to occur exactly once in a business process. Because of this characteristic, we capture information that is valid for the whole process within our model in this specific component.

Fork: This component can be used to represent a parallel process flow.

Join: The join element has the purpose to merge parallel flows into sequential flows. It is important to mention that this element is also responsible to get the flows ’synchronized’ before the process flow continues.

Decision: The decision component enables the representation of alternative task flows. The flow can be either influenced by a random variable or by attribute / variable conditions (e.g. stock > 50).

End: The end block indicates a possible process end.

8.1.2 Task elements

Sub-process: Processes can reach a rather high complexity. For that reason it can be useful to use subprocesses in order to break down the complexity per layer. From a modeler's perspective a subprocess can be seen as a normal process that can be integrated into another process model.

Activity: "An activity represents a unit of work performed by a user, system or partner. An activity may have some input and output and some associated actions (pre and post activity)."[30, p.2] For our purpose, an activity has to be described by the following attributes:

Table 8.2: Attributes of an activity within the meta-model

Name	Type	M/C	Description
ID	Integer	M	a unique identifier in order to enable simulation operations and analyzing steps
NAME	String	M	a readable name for the task. Has not to be unique.
COMPLETION FUNCTION	Longstring	M	a completion function describing the degree of completion related to time [101, p.8]
EXECUTION COSTS	Longstring	M	specifies the costs that arise when performing the activity
EXECUTION TIME	Time	M	provides information about the time that is needed to fulfill the task.

INTERRUPTIBLE	Enumeration	M	an attribute specifying whether the activity can be interrupted during execution (e.g. the review of a document can be easily interrupted and resumed at a later point in time without mentionable delays; on the other hand, the interruptions of some chemical tasks performed in a laboratory have to be carried out as a whole - otherwise the activity has to be restarted from the beginning). This value is of high importance when it comes to resource re-allocations. The default value is set to yes.
RTO	Time	C	According to the German Federal Office for Information Security the“... recovery time objective (RTO) specifies the time in which the process is intended to be recovered.”[12, p. 45]. In our model this time-period is relevant for analyzing whether tasks can be resumed within the planned time-frame.
MTPD	Time	C	The maximum tolerable period of disruption defines the time span during which an activity or service can be interrupted or unavailable before the company becomes damaged irreversibly. [16, p.13] In all design plans, special attention should be paid to not exceed this value.
CONFIDENTIALITY THRESHOLD	Float	M	A float number between 0 and 1 indicating the level of confidentiality that has to be guaranteed.
INTEGRITY THRESHOLD	Float	M	A float number between 0 and 1 indicating the level of integrity that has to be guaranteed.

AVAILABILITY THRESHOLD	Float	M	A float number between 0 and 1 indicating the level of availability that has to be guaranteed.
CONFIDENTIALITY	Float	M	current level of confidentiality
INTEGRITY	Float	M	current level of integrity
AVAILABILITY	Float	M	current level of availability
RESPONSIBLE	Interref	C	reference to a human resource or an organizational unit
CUSTOMER INTERFACE	Enumeration	C	This attribute provides information whether the activity has a direct interface to the customer. This is important as activities that have a high customer visibility are more likely to cause negative impacts on brand and reputation. Default is set to "No".
ACTIVITY RE-ALLOCATION RULE	Expression	C	Contains a re-allocation rule for an activity. The expression has to be formed as outlined in the formal model. Activity re-allocations can be seen as workarounds such as performing an automatic task manually. A typical example would be the processing of purchase orders. If the server for automatically providing a server is not available, a workaround could take new purchase orders by telephone.
COMMENT	String	C	A comment for verbal description of the activity.

8.1.3 Resource elements

The determination of value is a challenging task. A variety of factors exist that can be taken into consideration, such as the value that would be assigned by owners or users, the value competitors would pay for, replacement costs, acquisition costs, strategic value.[45, pp.86-87]

Resource:

Table 8.3: Attributes of a resource within the meta-model

Name	Type	M/C	Description
ID	Integer	M	a unique identifier in order to enable simulation operations and analyzing steps
NAME	String	M	a readable name for the task. Has not to be unique.
COSTS	Float	C	can be used either as an aggregated view on all costs or for other costs which do not fall into the categories acquisition, configuration, maintenance or replacement
ACQUISITION COSTS	Float	C	specifies the amount of money that was necessary to buy the resource
CONFIGURATION COSTS	Float	C	the amount of money needed to configure the resource
MAINTENANCE COSTS	Float	C	the costs of ongoing maintenance (per year)
REPLACEMENT COSTS	Float	M	the costs of replacement
REPLACEMENT TIME	Time	M	specifies the time in which the resource can be replaced
RECOVER COMPLEXITY	Enumeration	M	this attribute indicates whether a resource can be recovered if destroyed. Further it specifies in qualitative terms how complex a recovery of the resource would be.

RTO	Time	C	According to the German Federal Office for Information Security, the“... recovery time objective (RTO) specifies the time in which the process is intended to be recovered.”[12, p. 45]. In our model, this time-period is relevant for analyzing whether tasks can be resumed within the planned time-frame.
MTPD	Time	C	The maximum tolerable period of disruption defines the time span during which an activity or service can be interrupted or unavailable before the company becomes damaged irreversibly. [16, p.13]
MTTR	Time	C	mean time to repair
MTBF	Time	C	mean time between failure
CONFIDENTIALITY THRESHOLD	Float	M	A float number between 0 and 1 indicating the level of confidentiality that has to be guaranteed.
INTEGRITY THRESHOLD	Float	M	A float number between 0 and 1 indicating the level of integrity that has to be guaranteed.
AVAILABILITY THRESHOLD	Float	M	A float number between 0 and 1 indicating the level of availability that has to be guaranteed.
CONFIDENTIALITY	Float	M	current level of confidentiality
INTEGRITY	Float	M	current level of integrity
AVAILABILITY	Float	M	current level of availability
OWNER	Interref	C	reference to a human resource
RESTORATION DEPENDENCY	Longstring	C	specifies which other assets have to be in place before the resource can be functional again.
COMMENT	String	C	A comment for verbal description of the resource.

RESOURCE RE-ALLOCATION RULE	Expression	C	This element is solely for the re-allocation of resources. The expression within this field should at least consist of a Resource Attribute, Relational Operator, Threshold, Time Interval, Possible Replacement Options. For further details on the structure we kindly refer the reader to the formal model.

Employee: Beside the attributes mentioned in Table 8.3, the following characteristics are represented in our model.

Table 8.4: Attributes of a human resource element within the meta-model

Name	**Type**	**M/C**	**Description**
SKILL SET	Record	C	within our model it is possible to assign skills to human resources. This is especially useful for our resource allocation capabilities as resources with the similar skill set may carry out the same tasks as a deputy in the event of an emergency.
SECURITY CLEARANCES	Record	C	in order to analyze whether certain allocations might be feasible from an information perspective, it is essential to know the clearances of an employee. If this information is not available, security deficiencies could arise. For detailed information about clearances, we kindly refer the reader to [107]

WORKING SCHEDULE	Record	C	as human resources are only allowed to perform their tasks during working hours. Therefore this attribute specifies the standard working hours. Apart from that, compulsory or voluntary overtime hours can be defined.

Premise:

Table 8.5: Attributes of a physical resource element within the meta-model

Name	Type	M/C	Description
LOCATION	String	C	indicates where the physical resource is located (e.g., Vienna, Austria)
CLASSIFICATION	String	C	provides information about the classification of a room, premise or any other physical location

IT System:

Table 8.6: Attributes of a technical resource element within the meta-model

Name	Type	M/C	Description
CUSTODIAN	Interref	C	the responsible person to safeguard the asset
CLASSIFICATION	Enumeration	C	provides information about the classification of the asset

Information resource:

Table 8.7: Attributes of an information resource element within the meta-model

Name	Type	M/C	Description
CLASSIFICATION	String	C	provides information about the classification of the asset
CUSTODIAN	Interref	C	the responsible employee to safeguard the asset
USED IT SYSTEMS	Interref	C	indicates what systems are needed to access, store, distribute, dispose, ... the information
RPO	TIME	C	“ The target set for the status and availability of data [...] at the start of a recovery process.”[16, p.14]
MTDL	TIME	C	“The maximum loss of information [...] which an organization can tolerate.”[16, p.13]
STRATEGIC VALUE	Enumeration	C	indicates the strategic value of the information in qualitative terms
LOSS OF KNOWLEDGE	Enumeration	C	this attribute provides information (qualitative scale) about the knowledge loss that could result if the information asset gets destroyed.

Resource relation:

Table 8.8: Attributes of a resource relation element within the meta-model

Name	Type	M/C	Description
ID	Integer	M	a unique identifier in order to enable simulation operations and analyzing steps
NAME	String	M	a readable name for the element. Default is set to empty string ’ ’.

TYPE	Enumeration	M	can be either an ’AND’ or an ’OR’ relation. Default is set to ’AND’.
IS START RELATION	Enumeration	M	indicates whether the relation is the root of a specific resource relation.

Furthermore, to represent the organizational structure and to provide a high level overview of the organization’s risk situation, the following elements are introduced:

- Organizational unit: describes an organization or a part of an organization such as a department
- Role: describes a role that an employee can fulfill
- Business Objective: provides information about the aims of an organization
- Business Impact: assesses the impacts of a loss of availability, integrity or confidentiality on a high level
- Impact Scale: defines the scale and categories in which impacts should be captured

8.2 Extensions Enabling the Consideration of Risk Aspects

Figure 8.2 schematically outlines the relations between the main components of the Threat / Countermeasure Model which has evolved from [64, 60, 43, 102]

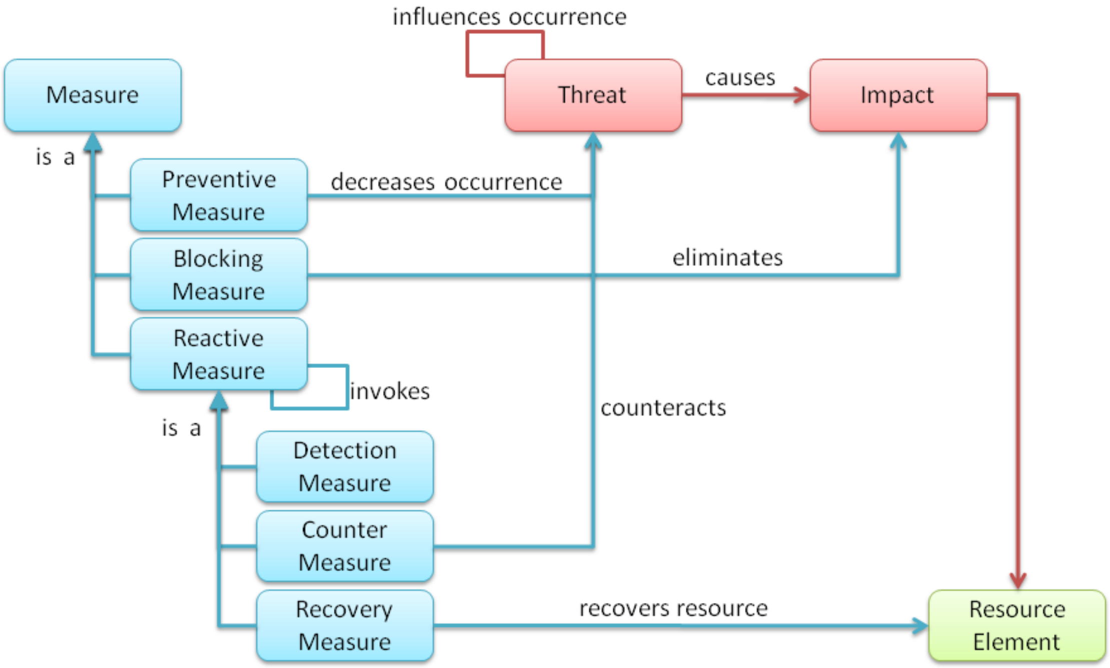


Figure 8.2: Threat / Countermeasure Model

Measure:

Table 8.9: Attributes of a measure element within the meta-model

Name	Type	M/C	Description
ID	Integer	M	a unique identifier in order to enable simulation operations and analyzing steps
NAME	String	M	a readable name for the element. Default is set to empty string ' '.

COSTS	Float	C	specifies the aggregated costs or other costs which are not separately mentioned
ACQUISITION COSTS	Float	C	specifies the amount of money that was necessary to buy the measure
CONFIGURATION COSTS	Float	C	the amount of money needed to implement and configure the resource
MAINTENANCE COSTS	Float	C	the costs of ongoing maintenance (per year)
CONFIDENCE	Enumeration	C	indicates the confidence level of information
COMMENT	String	C	A comment for verbal description of the measure.

Preventive Measure:

In this thesis, a preventive measure is a measure that reduces the probability of occurrence of a threat. An example is the use of flame-resistant textiles to reduce the probability of a fire threat.

Blocking Measure:

Blocking measures are safeguards that can immediately resolve a threat. An example of this type of measure is a malware filter.

Reactive Measure:

Reactive measures pursue the aim to model and simulate more complex and realistic measures. The three types of reactive measures are *Detection Measure*, *Counter Measure* and *Recovery Measure*. These types reflect the necessary phases to fight a threat.

Threat:

A threat can be described as something causing harm or damage to a resource or process. In our model, a threat is represented by the following attributes.

Table 8.10: Attributes of a threat element within the meta-model

Name	Type	M/C	Description

ID	Integer	M	a unique identifier in order to enable simulation operations and analyzing steps
NAME	String	M	a readable name for the element. Default is set to empty string ’ ’.
INTERVAL	TIME	C	the time interval in which the threat occurs
PROBABILITY	Float	C	the corresponding probability to the interval
CONFIDENCE	Enumeration	C	indicates the confidence level of information
COMMENT	String	C	A comment for verbal description of the measure.

Impact:

As a threat causes damage, an impact arises. In our model the impact is described by a function that negatively affects an attribute of a resource.

Table 8.11: Attributes of a threat element within the meta-model

Name	Type	M/C	Description
ID	Integer	M	a unique identifier in order to enable simulation operations and analyzing steps
NAME	String	M	a readable name for the element. Default is set to empty string ’ ’.
IMPACT FUNCTION	Expression	C	the impact function of a threat
RESOURCE ATTRIBUTE	String	C	the resource attribute that is impacted
CONFIDENCE	Enumeration	C	indicates the confidence of information
COMMENT	String	C	A comment for verbal description of the measure.

Resource:

The resource element contains an interref to an existing resource within the resource model.

Relations

The relation classes of the model describe how measures interact with threats as well as how a recovery measure restores the functionality of a resource.

8.3 Open Models Prototype

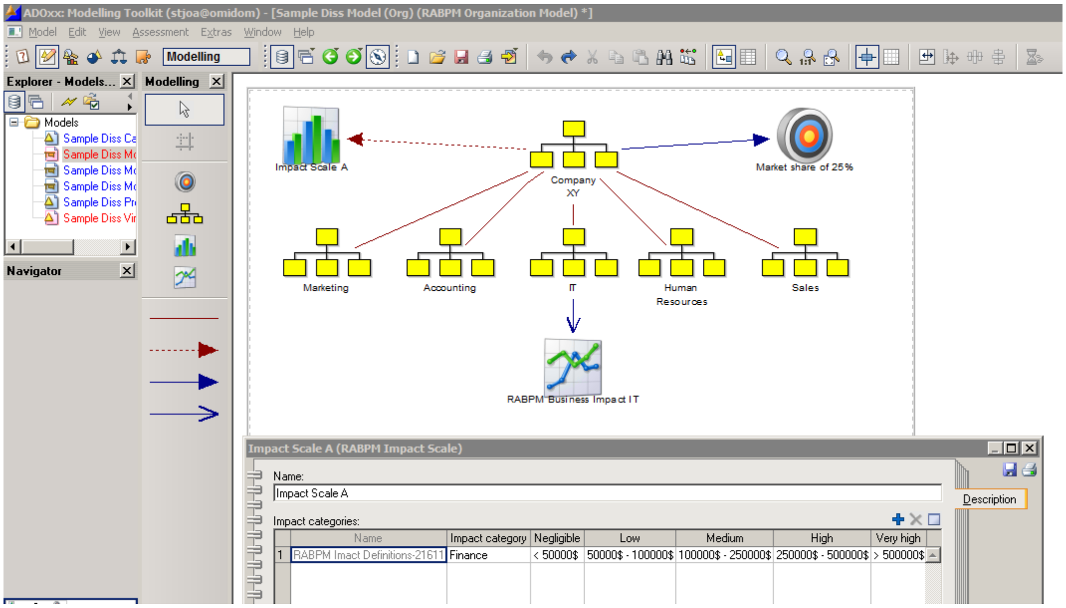
In this section we outline how our meta-model can be applied to facilitate the business continuity lifecycle. The presented implementation of the above-mentioned metamodel shall serve on the one hand as a toolkit for BCM / BR practitioners and on the other hand capture all the necessary data to conduct the planning of workarounds based on the formal model presented in the previous sections.

The central documents that have been considered when designing and evaluating the approach were frequently used and well-known BCM standards and best practices, especially BSI 100-4 [12], BS25999 [10, 11] and the BCI GPG [16]. Furthermore, the ADONIS modeling language has been a valuable input for deriving our model.

The starting point for our approach is the definition of the organization's structure. In our approach, this is performed via an adapted organization chart (RABPM Organization Model). The reason for this choice as the origin of our analysis steps is the high importance of an initial understanding of the importance and pertinence of individual parts of the company.

Beside the typical components of an organization chart, such as organizational units, roles/positions and employees, our organization chart holds information about the corresponding high level business objectives, impact categories (e.g. life/safety, finance, environment, reputation, ...) as well as likelihood and impact scales (i.e. what does a damage/harm of negligible, low, medium, high and very high mean for the impact categories). The determination of the core objectives is vital as all security ambitions shall support a business objective. The aims of a business or business unit strongly depend on the nature of the organization (e.g. non-profit vs profit-oriented organizations). Examples of typical business objectives are sales growth, extension of the product line-up or increase in market share. As described before, it is advantageous if the goals are described in a specific, measurable, attainable, relevant and time bound (SMART) way (see [76]). The likelihood and impact criteria are of high importance for the consistent analysis across whole organizations. For more information about risk criteria, we kindly refer to [4].

The following screenshot (Figure 8.3) highlights how our approach can be modeled using the OpenModels platform. In the figure one can see the organizational structure, the objective of the company and a first high-level picture about possible business impacts when loosing availability, integrity or confidentiality.



Impact Scale A (RABPM Impact Scale)

Name: Impact Scale A

Impact categories:

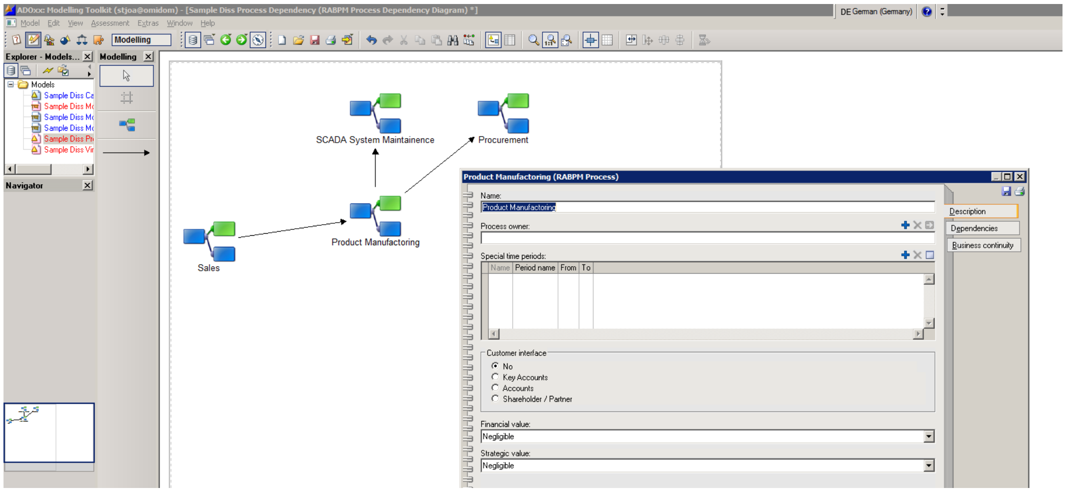
	Name	Impact category	Negligible	Low	Medium	High	Very high
1	RABPM Imact Definitions-21611	Finance	< 50000$	50000$ - 100000$	100000$ - 250000$	250000$ - 500000$	> 500000$

Figure 8.3: Prototype Screenshot: RABPM Organization Model with Notebook of Impact Scale Object

Within our model, business objectives are only described in a verbose manner. However, a beneficial extension of the model could be the design of a specific model with the aim to model business objectives in a comprehensive and consistent way ensuring at least the above-mentioned (SMART) attributes.

The process dependency model of our approach is similar to a process map with the special characteristic of highlighting the dependencies - under normal as well as under emergency conditions - between the processes. The consideration of dependencies under emergency conditions is of high importance for *business continuity response*. In addtion to the information about interdependencies and dependencies, the diagram provides information about the strategic, operational and financial value of a process on a high level. Furthermore, aspects such as process responsibilities, special time periods/peak periods and a high-level description of supply dependencies are captured by the diagram. For a closer look on risk-aware business process management and supply risk management we refer to [59].

Figure 8.4 shows a simple sample case for such a process dependency model. This model can also be used to define the initial scope of a BCM project.



Name: Product Manufactoring

Process owner:

Special time periods:

Name	Period name	From	To

Customer interface
● No
○ Key Accounts
○ Accounts
○ Shareholder / Partner

Financial value: Negligible

Strategic value: Negligible

Figure 8.4: Process Dependency Model

The business process model is the core component of business process management. It specifies the structure of a process. This comprises information on all activities as well as flow information such as information whether specific activities can be executed in parallel or information about decisions influencing the process flow. Figure 8.5 depicts a process model for the sample process presented in the previous Section 6.5.

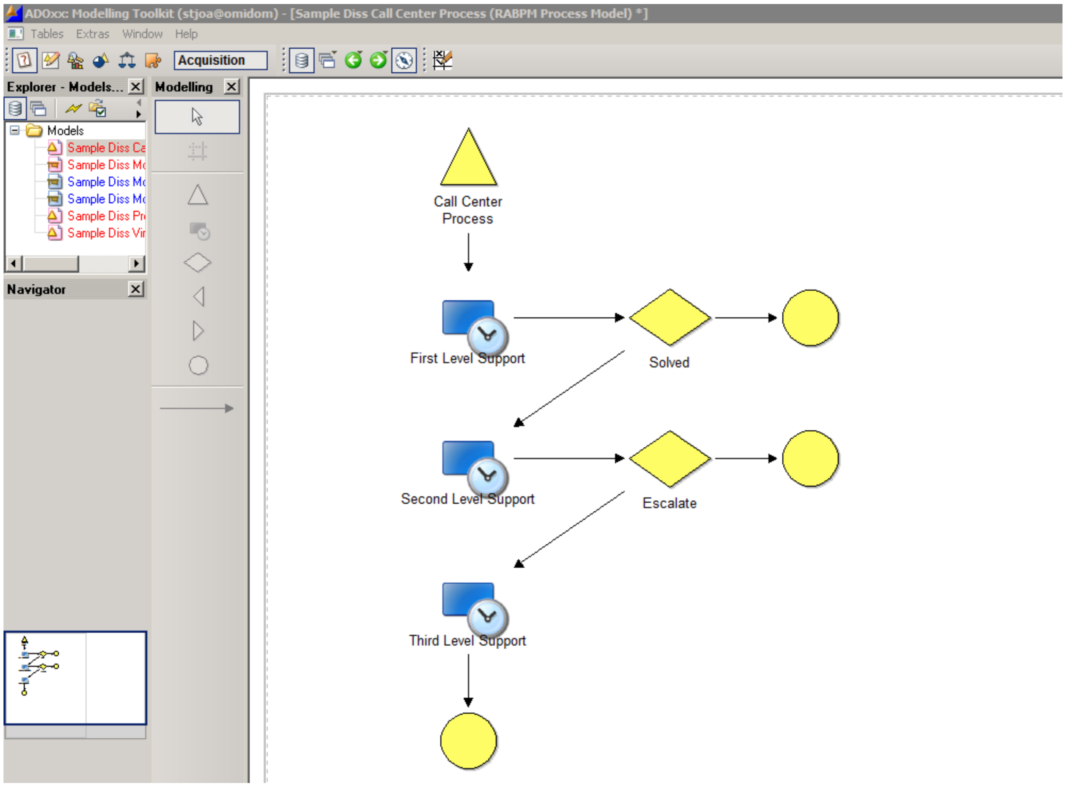
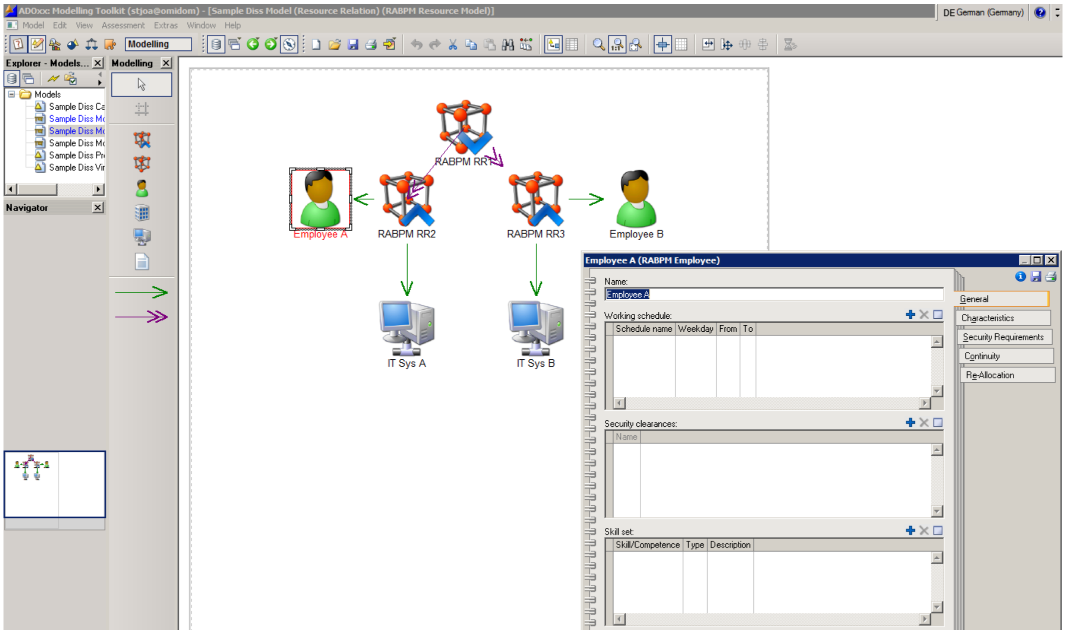


Figure 8.5: Process Model

In order to perform activities, resources are required. Therefore, we introduce our resource model which can be linked to activities. The resource model mainly consists of resource relations (i.e. AND relation / OR relation) as well as resources (i.e. Generic Resource, Employees, Premises, IT-Systems, Information Assets). In order to link the elements, we introduce two connectors. A complex connector that establishes the link between resource relations (purple connector) and a connector that links resource relations with resources (green connector). Figure 8.6 shows a corresponding resource model for the sample case.


ADOxx: Modelling Toolkit (stjoa@omidom) - [Sample Diss Model (Resource Relation) (RABPM Resource Model)]

Employee A (RABPM Employee)

Name: Employee A

Working schedule:

Schedule name	Weekday	From	To

Security clearances:

Name

Skill set:

Skill/Competence	Type	Description

Figure 8.6: Resource Relation Model

The last model to outline is the threat model. It provides details about a threat and its interdependencies with safeguards. The safeguarding elements can be divided into preventive measures (reducing the occurrence probability), blocking measures (eliminating the effects of a threat) as well as reactive measures (detecting and counteracting a threat as well as recovering damaged resources). As a threat can have multiple impacts on multiple resources and their corresponding attributes, we introduce an impact component.

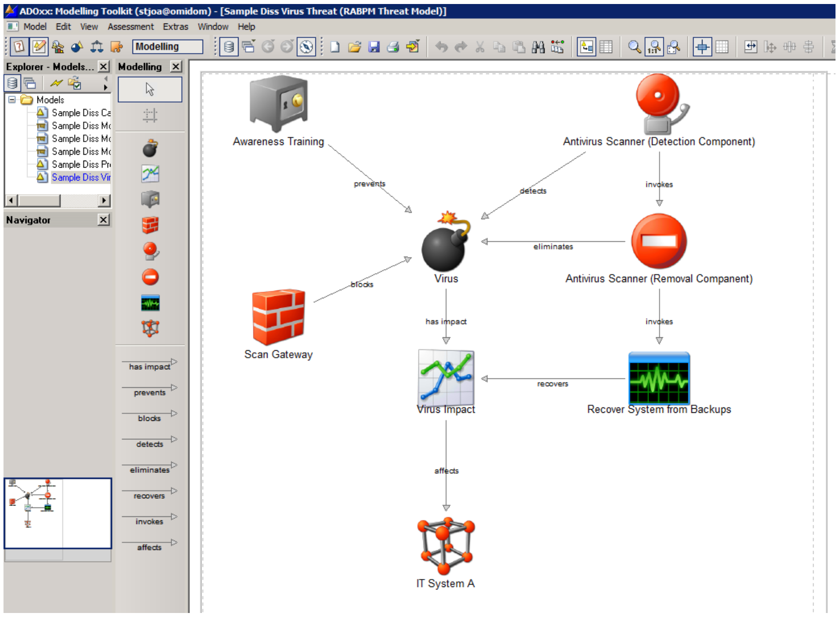


Figure 8.7: Threat Model

8.4 Chapter Summary

In this chapter we presented our OpenModels metamodel. We outlined the extensions and modifications required to a) facilitate the planning of workarounds and b) to support the methodological approach presented in the previous chapters of this thesis (see Section 6.1).

In the second part of this chapter, we presented the prototype implementation in OpenModels. Interested readers are welcome to download and adapt our approach at the Information Security Project Page of OpenModels (Project Risk Aware Business Process Management - http://www.openmodels.at/web/informationsecurity/home).

Part IV
Conclusion

Summary of major contributions, conclusions and indications for further work

> “There are two sides to every question.
>
> Protagoras

Incidents, crises and catastrophes are omnipresent in our daily headlines. Examples for such negative events are natural disasters (e.g. July floods in the UK in 2007, volcano Eyjafjallajoekull in 2010, earthquakes and tsunami in Japan in 2011), critical failures (e.g. power outages such as East Florida February in 2008), terrorist attacks (e.g. assault on the Atocha railway station in 2004, terrorist attacks on World Trade Center in 2001), data theft (e.g. Royal Navy 2008, Austrian Ministry of Justice 2005) or targeted attacks (e.g. Stuxnet).

Besides the incidents presented by the media, a huge variety of less spectacular threats exists that endangers the existence of companies. Examples of such threats are loss of key staff, loss of knowledge, disgruntled employees, insider threats or software failures. According to [49, 15], the vast majority of the crises affecting organizations are so called ’quiet catastrophes’ which are not reported by the media.

Business continuity pursues the aim to improve the resilience of organizations regardless of the negative event. Our focus lies on the design and implementation of robust structures that ensure proper response for large-scale incidents.

Various survey highlighted the importance of the subject. A survey conducted by the CMI states that “... 71 per cent of respondents claim that BCM is regarded as ’important’ or ’very important’ by senior management in their organisation ... ” [113, p.7]

Business continuity has its origins in the area of information technology. Today a trend can be seen from disaster recovery to an emerging discipline called "business resilience" which has a broader focus and concentrates on all areas of an organization. Elliot et al. [33] describe the reasons for this development as follows: "Organisations are socio-technical systems, and to manage them effectively for continuity, all elements must be considered" [33, p.3]

The key research questions answered by this thesis are:

- How can a method and/or framework combine security disciplines (such as business continuity) with business process management?
- How can this framework improve the planning phase of business continuity and security incident management by evaluating dynamic allocations of resources? What techniques are necessary to achieve this support?

The approach presented in this thesis contributes to the above-mentioned challenge by providing a common modeling language for business analysts, process owners, security and continuity experts.

The methodological approach assists continuity practitioners to build and maintain a business continuity management system. Risk-aware business process management is used as the foundation. The combination of modeling and simulation of business processes and security aspects (i.e. threats and detective, corrective and preventive countermeasures) enables the identification of mission critical resources, services, processes and dependencies. This distinction is of high importance as it is not feasible to secure all resources, services and processes to the same extent.

The extension of resource allocation modeling capabilities makes it possible to support the planning of workarounds and continuity responses. The usage of simulation can provide important background information for decision support on the effects of plans and measures such as cross-skill trainings. In order to improve the usability of the approach, we implemented our metamodel which supports the steps required to conduct this analysis (e.g. to get an initial understanding about dependencies amongst business processes, modeling threats, ...)

The core results of this thesis can be summarized as follows:

- A review of the state of the art: Within our literature review we firstly present several approaches focusing on the integration of security, risk and continuity aspects with business process management. This reflection on the one hand, supplies the reader with all necessary information required to have a good overview of the domain of risk aware business process management. On the other hand, the literature evaluation allows the reader to get an initial overview regarding business continuity planning and resource allocation strategies.

- An approach combining both, the business process management and business continuity perspective: In this thesis we show how concepts such as the BCM life cycle and the BPMS paradigm can be linked to generate an added value for the different target groups (e.g. business analysts, security analysts, ...) within an organization. This organizational consideration highlights how the approach fits into existing structures and is fundamental for the success of the method.

- A formal model that builds the foundation for our resource re-allocation considerations: The mathematical formulation of our conceptual model serves as a basis for our simulations. This solid foundation is essential to build reliable, understandable and comprehensible models. Furthermore, this specification facilitates the exchange within the research community.

- A Simulink prototype evaluating our formal model: The prototype artifact generated in this thesis provides details how an implementation of our formal model can be achieved using the widely-used software package Simulink.

- A metamodel: As the success of the whole approach depends on the acceptance of the users, we decided to build a metamodel that extends the formal model with information required by business analysts and continuity specialists. By introducing this metamodel we improve the usability and acceptance of the approach.

- Implementation of the metamodel in the OpenModels platform: The implementation of the metamodel within the OpenModels platform pursues the aim to allow a broad audience to use and access the created metamodel. This helps to disseminate the results achieved by this thesis. Furthermore, the decision to make the metamodel available through this platform allows research groups and practitioners to make their own adjustments where necessary and to eliminate existing limitations if required.

Currently, the major limitation of the approach is the high payload which is initially required in order to get meaningful results. Without the right level of modeling granularity, only results that provide a rough overview can be achieved. Such a high level may be sufficient for some first evaluation of the risk and impacts, but not for detailed planning of action.

Another challenge which remains unsolved is the estimation of probabilities of occurrence and the behavior of different risks. This is not a specific problem of the approach, but good risk estimations would considerably help to improve the final results of the approach.

The interdisciplinary field of business process management combined with security and business continuity has a huge range. We were obviously not able to tackle all relevant issues in this thesis. Therefore in the following paragraphs we will highlight further research areas that could be addressed to take the presented approach one step further.

One essential area of research would be the extension of the current modeling and simulation capabilities for risk analysis in critical infrastructure. The special characteristic of this research areas is that a special focus has to be laid on inter- and intra-domain interdependencies and dependencies.

Another important future work is the development of a comprehensive and common tool supporting the method. Currently, only extended proof-of-concept prototypes exist which were developed to evaluate our approach and test its feasibility. However, integrating the simulation capabilities into the OpenModel prototype and providing comprehensive report capabilities would help to improve usability and applicability.

Bibliography

[1] C. J. Alberts and A. J. Dorofee, "OCTAVE MethodImplementation Guide Version 2.0," Carnegie Mellon - Software Engineering Institute, Tech. Rep., 2001.

[2] ——, "Risk management framework," Carnegie Mellon University (CMU) - Software Engineering Institute (SEI), Tech. Rep., 2010.

[3] *Prudential Standard APS 232 - Business Continuity Management*, Australian Prudential Regulation Authority Std., 2005.

[4] *ONR49001 - Risk Management for Organisations and Systems*, Austrian Standards Organisation Std., 2010.

[5] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable Secur. Comput.*, vol. 1, pp. 11–33, January 2004. [Online]. Available: http://dx.doi.org/10.1109/TDSC.2004.2

[6] BBC. Japan earthquakes. http://www.bbc.co.uk/news/world-asia-pacific-12711226. Accessed April 19th, 2011. [Online]. Available: http://www.bbc.co.uk/news/world-asia-pacific-12711226

[7] W. Boehmer, C. Brandt, and J. F. Groote, "Evaluation of a business continuity plan using process algebra and modal logic," in *Proceedings of 2009 IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH),*. IEEE, 2009, pp. 147–152.

[8] F. Braber, I. Hogganvik, M. Lund, and F. V. K. Stolen, "Model-based security analysis in seven steps - a guided tour to the CORAS method," *BT Technology Journal*, vol. 25, pp. 101–117, 2007.

[9] R. Breu and F. Innerhofer-Oberperfler, "Model Based Business Driven IT Security Analysis," in *Proceedings of the Third Symposium on Requirements Engineering for Information Security (SREIS'05) held in conjunction with the 13th International Requirements Engineering Conference (RE'05)*, August 2005, pp. 921–928.

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

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

[12] BSI, *BSI Standard 100-4: Business Continuity Management*, German Federal Office for Information Security Std., 2009. [Online]. Available: https://www.bsi.bund.de/cae/servlet/contentblob/748954/publicationFile/41759/standard_100-4_e_pdf.pdf,AccessedAugust2011

[13] J. Burtles, *Principles and practice of business continuity*. Rothstein Associates Inc, 2007.

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

[15] Business Continuity Institute, "Good Practice Guidelines 2008 - A Management Guide to Implementing Global Good Practice in Business Continuity Management - Section 1: BCM POLICY & PROGRAMME MANAGEMENT," 2008. [Online]. Available: http://www.thebci.org/gpgdownloadpage.htm

[16] ——, "Good Practice Guidelines 2010 - A Management Guide to Implementing Global Good Practice in Business Continuity Management - Global Edition," 2010. [Online]. Available: http://www.thebci.org/gpgdownloadpage.htm

[17] CA Technologies, "RESEARCH REPORT: THE AVOIDABLE COST OF DOWNTIME," CA Technologies, Tech. Rep., 2010.

[18] R. A. Caralli, J. H. Allen, P. D. Curtis, D. W. White, and L. R. Young, "CERT- Resilience Management Model, Version 1.0 Process Areas, Generic Goals and Practices, and Glossary," CERT, Tech. Rep., 2010.

[19] ——, "Improving Operational Resilience Processes: The CERT Resilience Management Model," in *IEEE Second International Conference on Social Computing (SocialCom 2010)*, 2010.

[20] CERT. Resilience management. http://www.cert.org/resilience/, accessed June 2011. CERT.

[21] ——. (2009) OCTAVE. [Online]. Available: http://www.cert.org/octave

[22] R. Chen, R. Sharman, H. R. Rao, and S. Upadhyaya, "Design principles for critical incident response systems," *Information Systems and E-Business Management*, vol. 5, pp. 201 – 227, 2007.

[23] CLUSIF (Club de la Securite de l'Information Francais). Mehari 2010 documents. http://www.clusif.asso.fr/en/clusif/present/, accessed May 2011.

[24] ——, "Business continuity plan - is strategy and recovery solutions," CLUSIF, Tech. Rep., 2004.

[25] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004) Enterprise risk management: Executive summary. [Online]. Available: http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

[26] A. De Korvin, S. Hashemi, G. Quirchmayr, and K. R., "Assigning tasks to resource pools: A fuzzy set approach," in *LNCS of the DEXA Conference (DEXA2000)*, 2000.

[27] W. E. Deming, *Out of the crisis*. MIT Press, 1986.

[28] M. Dey, "Business Continuity Planning (BCP) methodology - Essential for every business," in *Proceedings of GCC Conference and Exhibition*. IEEE, 2011, pp. 229 – 232.

[29] Disaster Recovery Journal and DRI International. (2007, 08) Generally accepted practices for business continuity practitioners.

[30] J.-J. Dubray, "A novel approach for modeling business process definitions," EBPML.ORG, Tech. Rep., 2002. [Online]. Available: http://www.ebpml.org/ebpml2.2.doc

[31] 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)*, 2009, pp. 1–10.

[32] ——, "Ontology-based decision support for information security risk management," in *International Conference on Systems (ICONS 2009)*, 2009, pp. 80–85.

[33] D. Elliot, E. Swartz, and B. Herbane, *Business Continuity Management - A Crisis Management Approach*, 2nd ed. Routledgt, 2010.

[34] ENISA, "It business continuity management - an approach for small medium sized organizations," European Network and Information Security Agency (ENISA), Tech. Rep., 2010.

[35] C. Ericson, "Fault tree analysis - a history," in *Proceedings of the 17th International System Safety Conference*, 1999.

[36] European Commission, "Auditing directives."

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

[38] D. Everest, R. E. Garber, and M. K. B. Peterson, "Gtag (global technology audit guide) - business continuity management," IIA, Tech. Rep., 2008.

[39] 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)*, 2009, pp. 113–127.

[40] ——, “Information security risk management: In which security solutions is it worth investing,” *Communications of the Association for Information Systems*, vol. 28, pp. 329 – 356, 2011.

[41] Gartner Inc. (2009) Gartner exp worldwide survey of more than 1.500 cios shows it spending to be flat in 2009. http://www.gartner.com/it/page.jsp?id=855612. [Online]. Available: http://www.gartner.com/it/page.jsp?id=855612

[42] J. Gilbert, “Business continuity management legislations, regulations and standards version 6, january 2011,” Business Continuity Institute, Tech. Rep., 2011.

[43] 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 International Conference on Systems Science (HICSS-41 2008)*, 2008, p. 377.

[44] G. Governatori and Z. Milosevic., “A formal analysis of a business contract language,” *International Journal of Cooperative Information Systems*, vol. 15, no. 4, pp. 659–685, 2006.

[45] S. Harris, *CISSP Certification All-in-One Exam Guide, Fourth Edition*, 4th ed. McGraw-Hill Osborne Media, 11 2007. [Online]. Available: http://amazon.com/o/ASIN/0071497870/

[46] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design science in information systems research,” *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004.

[47] Z. Huang, W. van der Aalst, X. Lu, and H. D. a, “Reinforcement learning based resource allocation in business process management,” *Data & Knowledge Engineering*, vol. 70, pp. 127–145, 2011.

[48] ICM Computer Group. Beginners guide to business continuity. [Online]. Available: http://www.continuitycentral.com/BCMBASICS.pdf,accessedMay2011

[49] ICM COMPUTER GROUP, “Beginners guide to business continuity,” ICM COMPUTER GROUP, Tech. Rep.

[50] *IEEE Std 1490(TM)-2003: IEEE Guide - Adoption of PMI Standard - A Guide to the Project Management Body of Knowledge*, IEEE Std., 2003.

[51] International Organization for Standardization, “Iso/iec 24762:2008 information technology - security techniques - guidelines for information and communications technology disaster recovery services,” ISO/IEC, 2008.

[52] ISACA. (2011) Cisa glossary. [Online]. Available: http://www.isaca.org/Knowledge-Center/Documents/Glossary/cisa_glossary.pdf,AccessedAugust2011

[53] ——, *CISM Review Manual 2011*, ISACA, Ed. ISACA, 2011.

[54] *ISO/IEC Guide 73:2002 Risk management – Vocabulary – Guidelines for use in standards*, ISO/IEC Std., 2002.

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

[56] *ISO 31010:2009 - Risk management - Risk assessment techniques*, ISO/IEC Std., 2009.

[57] *ISO/PAS 22399:2007: Societal security - Guideline for incident preparedness and operational continuity management*, ISO/PAS Std., 2007.

[58] S. Jakoubi, S. Tjoa, G. Goluch, and Q. G., "A survey of scientific approaches considering the integration of security and risk aspects into business process management," in *International Workshop on Business Processes Security (BPS2009)*. IEEE, 2009.

[59] S. Jakoubi, "Improving service level management by introducing risk-aware service level analysis and planning using risk-aware business process management," unpublished Work - Disseration not finished at the time of publication.

[60] 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.

[61] 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.

[62] 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, 2009.

[63] S. Jakoubi, S. Tjoa, S. Goluch, and G. Kitzler, "A formal approach towards risk-aware service level analysis and planning," in *Fifth International Conference on Availability,Reliability and Security (ARES 2010)*, 2010, pp. 180–187.

[64] 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.

[65] A. Jallow, B. Majeed, K. Vergidis, A. Tiwari, and R.Roy, "Operational risk analysis in business processes," *BT Technology Journal*, vol. 25, pp. 168–177, 2007.

[66] M. Jensen and S. Feja, “A security modeling approach for web-service-based business processes,” in *16th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems (ECBS 2009)*, 2009.

[67] S. Junginger, H. Kühn, R. Strobl, and D. Karagiannis, “Ein geschäftsprozessmanagement-werkzeug der nächsten generation -adonis: Konzeption und anwendungen [available only in german],” University of Vienna / BOC GmbH, Tech. Rep., 2000. [Online]. Available: http://stefanjunginger.com/mediapool/99/998477/data/Junginger_et_al._-_Ein_Geschaefts..._-_BPMS-Bericht_-_200011.pdf,AccessedApril2011

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

[69] 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*, 2007, pp. 315–321.

[70] D. Karagiannis, “Bpms: business process management systems,” *SIGOIS Bull.*, vol. 16, pp. 10–13, August 1995. [Online]. Available: http://doi.acm.org/10.1145/209891.209894

[71] D. Karagiannis, W. Grossmann, and P. Höfferer, “Open model initiative - a feasibility study,” University of Vienna, Tech. Rep., 2007. [Online]. Available: http://www.openmodels.at/web/omi/press

[72] K. Khanmohammadi and S. H. Houmb, “Business process-based information security risk assessment,” in *Proceedings of the 2010 Fourth International Conference on Network and System Security*, ser. NSS ’10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 199–206. [Online]. Available: http://dx.doi.org/10.1109/NSS.2010.37

[73] R. F. Knight and D. J. Pretty, “The impact of catastrophes on shareholder value,” Templeton College, University of Oxford, Tech. Rep., 1996.

[74] London Resilience Partnership / UK Government . London resilience team | business continuity | home. http://www.londonprepared.gov.uk/businesscontinuity/, accessed June 2011.

[75] J. Maddox. (2010, September) CNN. [Online]. Available: http://articles.cnn.com/2010-09-24/tech/stuxnet.computer.malware_1_malware-computers-machine?_s=PM:TECH,April2011

[76] P. J. Meyer. What would you do if you knew you couldn’t fail? creating s.m.a.r.t. goals. www.oma.ku.edu/soar/smartgoals.pdf, August 2011.

[77] Microsoft Corporation, “The security risk management guide,” Microsoft Corporation, Tech. Rep., 2006.

[78] National Fire Protection Association, “Nfpa 1600:2007 - standard on disaster/emergency management and business continuity programs,” 2007.

[79] National Institute of Standards and Technology, “NIST SP800-34: Contingency Planning Guide for Information Technology Systems,” 2002.

[80] ——, “Nist special publication 800-30, risk management guide fir information technology systems,” National Institute of Standards and Technology (NIST), 2002.

[81] ——, “Nist sp800-61: Computer security incident handling guide,” National Institute of Standards and Technology, 2004.

[82] ——, “Nist special publication 800-37 - guide for applying the risk management framework to federal information systems,” http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf, accessed May 2011, National Institute of Standards and Technology (NIST), 2010 Rev.1.

[83] ——, “Nist special publication 800-39 - managing information security risk: Organization, mission, and information system view,” http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf, accessed May 2011, National Institute of Standards and Technology (NIST), 2011.

[84] D. Neiger and L. Churilov, “Goal-oriented and business process modeling with epcs and value-focused thinking,” in *Proceedings of Business Process Management (BPM 2004)*, 2004.

[85] 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.

[86] M. Netjes, W. M. van der Aalst, and H. A. Reijers, “Analysis of resource-constrained processes with colored petri nets,” in *Sixth Workshop and Tutorial on Practical Use of Coloured Petri Nets and the CPN Tools*, 2005.

[87] B. News. (2010) Volcanic ash: Europe flights grounded for third day. http://news.bbc.co.uk/2/hi/8626505.stm, accessed May 2011.

[88] One Hundred Seventh Congress of the United States of America, “Sarbanes-oxley act,” 2002.

[89] D. Ouelhadj and S. Petrovic, “A survey of dynamic scheduling in manufacturing systems,” *Journal of Scheduling*, vol. 12, pp. 417–431, 2009, 10.1007/s10951-008-0090-8. [Online]. Available: http://dx.doi.org/10.1007/s10951-008-0090-8

[90] A. Refsdal and K. Stolen, “Employing key indicators to provide a dynamic risk picture with a notion of confidence,” in *Trust Management III. Third IFIP WG 11.11 International Conference (IFIPTM 2009)*. Springer, 2009, pp. 215–233.

[91] A. Rodriguez, E. Fernandez-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)*, 2006, pp. 51–61.

[92] N. Russell and W. M. van der Aalst, “Work distribution and resource management in bpel4people: Capabilities and opportunities,” in *Proceedings of 20th International Conference on Advanced Information Systems Engineering*. Springer, 2008.

[93] N. Russell, W. M. van der Aalst, A. H. ter Hofstede, and D. Edmond, “Workflow resource patterns: Identification, representation and tool support,” in *Proceedings of 20th International Conference on Advanced Information Systems Engineering*. Springer, 2005.

[94] S. Sackmann, “A reference model for process-oriented it risk management,” in *16th European Conference on Information Systems*, 2008.

[95] S. Sadiq, G. Governatori, and K. Namiri, “Modelling control objectives for business process compliance,” in *5th International Conference on Business Process Management (BPM2007)*, 2007, pp. 149–164.

[96] A.-W. Scheer and M. Nüttgens, “ARIS Architecture and Reference Models for Business Process Management,” in *Business Process Management, Models, Techniques, and Empirical Studies*. London, UK: Springer-Verlag, 2000, pp. 376–389. [Online]. Available: http://portal.acm.org/citation.cfm?id=647778.734910

[97] A. Sienou, E. Lamine, and H. Pingaud, “A method for integrated management of process-risk,” in *1st International Workshop on Governance, Risk and Compliance - Applications in Information Systems (GRCIS’08)*, 2008.

[98] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, and D. Lynes, “Nist special publication 800-34 rev. 1 - contingency planning guide for federal information systems,” National Institute of Standards and Technology (NIST), 2010.

[99] The Business Continuity Institute (BCI). (2010) Good practice guidelines. [Online]. Available: http://www.thebci.org/gpg.htm

[100] S. Tjoa. (2011) Open models initiative - information security init. http://www.openmodels.at/web/informationsecurity/home, accessed 2011.

[101] S. Tjoa, S. Jakoubi, G. Goluch, G. Kitzler, S. Goluch, and G. Quirchmayr, “A formal approach enabling risk-aware business process modeling and simulation,” *IEEE Transactions on Services Computing*, vol. 4, no. 2, pp. 153–166, 2011.

[102] 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*, 2008, pp. 48–55.

[103] S. Tjoa, S. Jakoubi, S. Goluch, and G. Kitzler, “Planning dynamic activity and resource allocations using a risk-aware business process management approach,” in *Fifth International Conference on Availability, Reliability and Security (ARES 2010)*, 2010, pp. 268–274.

[104] 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*, 2008, pp. 179–186.

[105] H. Topcuoglu, S. Hariri, and M.-Y. Wu, “Performance-effective and low-complexity task scheduling for heterogeneous computing,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 13, pp. 260 – 274, 2002.

[106] A. Tsalgatidou and S. Junginger, “Modelling in the re-engineering process,” *SIGOIS Bull.*, vol. 16, pp. 17–24, August 1995. [Online]. Available: http://doi.acm.org/10.1145/209891.209896

[107] U.S. DEPARTMENT OF ENERGY , *DOE M 470.4-5 - Personnel Security*, U.S. DEPARTMENT OF ENERGY , 2005. [Online]. Available: www.directives.doe.gov

[108] W. M. van der Aalst, M. Rosemann, and M. Dumas, “Deadline-based escalation in process-aware information systems,” *Decision Support Systems*, vol. 43, pp. 492 – 511, 2007.

[109] C. Wang, Q. Tian, X. Chen, and C. Ying, “Service differentiation for business process by value based service scheduling,” in *In Proceedings of 2008 IEEE International Conference on Web Services*, 2008.

[110] 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.

[111] M. Weske, *Business Process Management: Concepts, Languages, Architectures*. Springer, 2007.

[112] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek, “Handbook for Computer Security Incident Response Teams (CSIRTs) - 2nd edition,” Carnegie Mellon - Software Engineering Institute, Tech. Rep., 2003.

[113] P. Woodman and P. Hutchings, “Disruption & resilience - the business continuity management survey 2010,” Chartered Management Institute (CMI), Tech. Rep., 2010.

[114] ——, “Managing threats in a dangerous world,” Chartered Management Institute, Tech. Rep., 2011.

[115] P. Woodman and V. Kumar, “A decade of living dangerously - the business continuity management report 2009,” Chartered Management Institute, Tech. Rep., 2009.

[116] J. Xu, C. Liu, and X. Zhao, “Resource allocation vs. business process improvement: How they impact on each other,” in *6th International Conference on Business Process Management*. Springer, 2008.

[117] A. Zalewski, P. Sztandera, M. Ludzia, and M. Zalewski, “Modeling and analyzing disaster recovery plans as business processes,” in *Computer Safety, Reliability, and Security*, ser. Lecture Notes in Computer Science, M. Harrison and M.-A. Sujan, Eds. Springer Berlin / Heidelberg, 2008, vol. 5219, pp. 113–125. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-87698-4_12

[118] Y. Zhou and Y. Chen, “Project-oriented business process performance optimization,” in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, 2003, pp. 4079–4084.

[119] M. zur Muehlen and M. Rosemann, “Integrating risks in business process models,” in *Australasian Conference on Information Systems (ACIS 2005)*, 2005.

List of Figures

List of Tables

Part V

Appendices

Glossary and Abbreviations

Name	Description
APS	Australian Prudential Standard
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BIA	Business Impact Analysis
BPE	Business Process Elements
BPM	Business Process Management
BPMS	Business Process Management System
BR	Business Resilience
CERT	Computer Emergency Response Team
CMI	Chartered Management Institute
CPN	Colored Petri Nets
DR	Disaster Recovery
EPC	Event-Driven Process Chains
ISO	International Organization for Standardization
ISRM	Information Security Risk Management
MTBF	Mean Time Between Failure
MTPD	Maximum Tolerable Period of Disruption
MTTR	Mean Time To Repair
NIST	National Institute of Standards and Technology
RMM	CERT Resilience Management Model
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCADA	Supervisory Control and Data Acquisition
SMART	Specific, Measurable, Attainable, Relevant and Time bound
SOA	Service Oriented Architecture
SOX	Sarbanes Oxley Act
UML	Unified Modeling Language

Curriculum Vitae

Name	Simon Tjoa
Degree	Master of Business Informatics
Job Title	University Lecturer
Nationality	Austrian
Date of Birth	April 28th, 1981
Gender	Male
Address	Kreuzbrunn 15E/4 3001 Mauerbach
Mobile	++43 660 346 343 0
Email	Phd [-@-] Tjoa.at

Education

Since 2006	PhD studies (Informatics), University of Vienna
1999 – 2006	Business Informatics University of Vienna, academic title Mag. rer. soc. oec.
1991 – 1999	High School with graduation, Gymnasium Neulandschule, 1190 Vienna
1987 – 1991	Elementary school Albrechtsschule, Klosterneuburg

Professional Experience

Since 08/2009	**St. Pölten University of Applied Sciences** Module manager (Information Security Management Module) University lecturer Senior researcher Equal opportunities representative (11/2011)
Since 2006	**ARES Conference**, http://www.ares-conference.eu (International Conference on Availability, Reliability and Security) Member of the organizing committee
2007 – 2010	**Security Research**, http://www.securityresearch.at Security Consultant
2007 – 2010	**CISIS Conference**, (International Conference on Complex, Intelligent and Software Intensive Systems) Member of the organizing committee
2006 – 2010	**Secure Business Austria,** http://www.sba-research.org Researcher / Security Consultant
2003 – 2010	**Freelancer** Software Development Projects, Consulting Projects
1997 – 2007	**DEXA Conference**, http://www.dexa.org (International Conference on Database and Expert Systems Applications) Member of the organizing committee
07/2006 – 08/2006	**University of South Australia** Guest lecturer
02/2005 – 06/2005	**University of Vienna** Tutor
2000 – 2003	**CSP (Computer Software Production),** http://www.csp.at Technical Analyst

Language Skills

German	Native fluency
English	Good fluency
French	Beginner
Polish	Beginner

Certifications

AccessData Certified Examiner (ACE)
ADONIS Process Manager Certificate
Associate Member Certificate of the Business Continuity Institute (AMBCI)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
ITIL v2 Foundation Certificate
Reuters 3000 Xtra
Symantec Data Loss Prevention Specialist
Further education of computer didactics in the context of the "GO-ON – Österreich ans Internet" initiative of the Austrian Government with the certification as internet trainer

List of publications

2011

Poisel, R., Tjoa, S., Tavolato, P.(2011) Advanced File Carving Approaches for Multimedia Files, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol. 2, No. 4

Poisel, R., Tjoa, S. (2011) Forensics Investigations of Multimedia Data: A Review of the State-of-the-Art. In: Proceedings of the 6th International Conference on IT Security Incident Management & IT Forensics, IEEE Computer Society

Poisel, R., Tjoa, S. (2011) Roadmap to Approaches for Carving of Fragmented Multimedia Files. In: Proceedings of The Fourth International Workshop on Digital Forensics (WSDF'11), IEEE

Tjoa, S., Jakoubi, S., Goluch, G., Kitzler, G., Quirchmayr, G. (2011) A Formal Approach Enabling Risk-aware Business Process Modeling and Simulation. IEEE Transactions on Services Computing, 4(2), IEEE

Tjoa, S. Poisel, R. (2011) A reference architecture for a scalable digital forensics toolkit. In: 5. Forschungsforum der Österreichischen Fachhochschulen, Wien, Austria. FH Campus Wien.

2010

Jakoubi S., Tjoa S., Goluch S. , Kitzler G. (2010) Risk-Aware Business Process Management—Establishing the Link Between Business and Security, Complex Intelligent Systems and Their Applications, Springer Optimization and Its Applications, 2010, Volume 41, 109-135, Springer

Jakoubi S., Tjoa S., Kitzler G., Goluch S. (2010) A Formal Approach Towards Risk-Aware Service Level Analysis and Planning, Full Paper, International Conference on Availability, Reliability and Security (ARES 2010), IEEE

Tjoa S., Jakoubi S., Kitzler G., Goluch S. (2010) Planning Dynamic Activity and Resource Allocations Using a Risk-Aware Business Process Management Approach, Short Paper, International Conference on Availability, Reliability and Security (ARES 2010), IEEE

2009

Neubauer T., Goluch G., Jakoubi S., Tjoa S., Wisser M. (2009) A Process Model for RFID based Business Process Analysis, IEEE Asia Pacific Services Computing Conference 2009 (APSCC), IEEE

Jakoubi S., Tjoa S. (2009) A Reference Model for Risk-Aware Business Process Management, International Workshop on Secure Service Computing (SSC), IEEE

Huber M., Kowalski S., Nohlberg M., Tjoa S. (2009) Towards Automating Social Engineering Using Social Networking Sites, IEEE International Conference on Information Privacy, Security, Risk and Trust, IEEE

Jakoubi S., Tjoa S., Goluch, G., Quirchmayr, G. (2009) A Survey of Scientific Approaches Considering the Integration of Security and Risk Aspects into Business Process Management, International Workshop on Business Processes Security, IEEE

2008

Tjoa, S., Jakoubi, S., Quirchmayr, G. (2008) Enhancing Business Impact Analysis and Risk Assessment applying a Risk-Aware Business Process Modeling and Simulation Methodology, in ARES, 3rd International Conference on Availability, Reliability and Security, IEEE

Tjoa, S., Jakoubi, S., Goluch, G., Quirchmayr, G. (2008) Extension of a Methodology for Risk-Aware Business Process Modeling and Simulation Enabling Process-Oriented Incident Handling Support, in AINA, 22nd International Conference on Advanced Information Networking and Applications , IEEE

Goluch, G., Ekelhart, A., Fenz, S., Jakoubi, S., Tjoa, S., Mück, T. (2008) Integration of an Ontological Information Security Concept in Risk-Aware Business Process Management, in HICSS, 41st Hawaii International Conference on System Sciences, IEEE

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

2007

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

Goluch, G., Ekelhart, A., Fenz, S., Jakoubi, S, Riedl, B., Tjoa, S. (2007) CASSIS - Computer-based Academy for Security and Safety in Information Systems, in ARES, 2nd International Conference on Availability, Reliability and Security, IEEE

Personal Interests

Cooking
Karate
Travelling
Volleyball