TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

Diploma Thesis

The Definition of Secure Business Processes with Respect to Multiple Objectives

Johannes Heurix
Koppstraße 6/1/2/8
1160 Wien

Supervised by
Prof. Dipl.-Ing. Dr. A Min Tjoa
Dipl.-Ing. Mag. Dr. Thomas Neubauer

Institute for Software Technology and Interactive Systems
Vienna University of Technology

Vienna, November 26, 2007

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die vorliegenden Quellen nicht benützt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Wien, 26. November 2007 Johannes Heurix

Danksagung

Zunächst möchte ich mich bei meinem Betreuer Dr. Thomas Neubauer für die fachliche Unterstützung und die gute Zusammenarbeit bedanken. Weiters möchte ich meinen Eltern und meiner Familie für ihre moralische und vor allem finanzielle Unterstützung danken, welche mir das Studium überhaupt erst ermöglicht hat. Des weiteren gilt mein Dank meinen Freunden Karin und Stephan, die mich durch einige Bemerkungen auf interessante Ideen brachten, und besonders der Sigi, die trotz ihres engen Terminkalenders die Zeit gefunden hat, meine Arbeit korrekturzulesen.

Abstract

Business processes have gained more and more importance in today's business environment, and their unimpeded execution is crucial for a company's success. Since business processes are permanently exposed to several threats, organizations are forced to pay attention to security issues. Although security of business activities is widely considered as important, business processes and security aspects are often developed separately. Recent approaches for managing business process security focus on certain aspects only and neglect others, thus not providing a holistic framework for analyzing process security and evaluating security safeguards. Often, these safeguards are evaluated according to technical aspects only; multiple objectives are not considered.

This diploma thesis introduces a model-supported, risk-based multiobjective decision making methodology (MR-MOD) for the elicitation of security requirements of business processes, for the analysis of assets, threats, and vulnerabilities, and for the selection of appropriate security technologies. Thereby it combines the strengths of different methods, including process modeling, quantitative risk assessment, and multiobjective decision making techniques, for the definition of Secure Business Processes. MR-MOD is supported by the MODStool, a software application developed in the course of this thesis. Finally, the feasibility of this methodology is demonstrated in a case study.

By combining different techniques, all aspects of evaluating safeguards to define Secure Business Processes can be taken into account: Using process models as the basis for the evaluation, decision makers can focus on the core processes of their company. The quantitative risk assessment, defined as a workshop process to allow for multiple persons to participate, provides a structured way to evaluate the safeguards' effectiveness in mitigating risks. And multiobjective decision making techniques ensure that factors other than the safeguards' risk mitigating capability are considered as well.

Kurzfassung

Im heutigen Geschäftsumfeld gewinnen Geschäftsprozesse mehr und mehr an Bedeutung und deren ungestörter Ablauf ist entscheidend für den Erfolg eines Unternehmens. Da Geschäftsprozesse permanent mehreren Gefahren ausgesetzt sind, sind Organisationen dazu gezwungen sicherheitsrelevanten Problemen Bedeutung beizumessen. Obwohl die Sicherheit von Geschäftstätigkeiten allgemein für wichtig erachtet wird, werden Geschäftsprozesse und Sicherheitsaspekte häufig getrennt voneinander entwickelt. Gegenwärtige Ansätze zur Gewährleistung der Sicherheit von Geschäftsprozessen richten ihr Hauptaugenmerk nur auf bestimmte Aspekte und vernachlässigen dadurch andere. Folglich stellen sie keine ganzheitliche Methodik dar, um die Sicherheit von Prozessen zu analysieren und um Sicherheitsmaßnahmen zu evaluieren. Oft werden diese nur nach technischen Gesichtspunkten bewertet, mehrfache Kriterien bleiben weitgehend unberücksichtigt.

Diese Diplomarbeit stellt eine Methodik zur modellunterstützten und risikobasierten Multikriteriellen Entscheidungsfindung (MR-MOD) vor, die zur Erhebung von Sicherheitsanforderungen von Geschäftsprozessen, zur Analyse von Wertanlagen, Bedrohungen und Schwachstellen und zur Auswahl von geeigneten Sicherheitstechnologien herangezogen werden kann. Dabei verbindet sie die Stärken verschiedener Methoden zur Definition von sicheren Geschäftsprozessen, darunter Prozessmodellierung, Risikobewertung und Techniken der Multikriteriellen Entscheidungsfindung. MR-MOD wird durch die Softwareapplikation MODStool unterstützt, welche im Rahmen dieser Arbeit entwickelt wurde. Schließlich wird die Machbarkeit dieser Methodik anhand einer Fallstudie demonstriert.

Durch die Kombination von mehreren Techniken können alle Aspekte für die Definition von sicheren Geschäftsprozessen berücksichtigt werden: Indem Prozessmodelle als Basis für die Evaluierung herangezogen werden, können sich die Entscheidungsträger auf die Kernprozesse ihrer Unternehmen konzentrieren. Die quantitative Risikobewertung, welche als Workshop definiert ist um es mehreren Personen zu ermöglichen teilzunehmen, ermöglicht eine strukturierte Bewertung der Effektivität von Sicherheits-

maßnahmen zur Risikoverringerung. Und die Techniken der Multikriteriellen Entscheidungsfindung gewährleisten es, dass auch andere Faktoren außer der Risikominderung berücksichtigt werden.

Contents

List of Figures

List of Tables

1. Introduction

1.1. Motivation

Since the shift from a 'functional' to a 'process-centered' view of business activities began in the 1980s [HM99], business processes have played a major role in today's business environment. Business Process Management (BPM) is applied to "analyse and continually improve fundamental activities such as manufacturing, marketing, communications and other major elements of a company's operations" [Zai97], or, in other words, to engineer lean and streamlined business processes [HM99]. The introduction of BPM has several benefits including Cost Reduction, Quality Improvements and Error Reduction, Visibility Gain, Process Step Automation, and Satisfaction Improvements [HWHL03].

In recent times, business processes have often been the target of a number of security hazards such as viruses, hacker attacks, or data theft [NKB06]. Given the importance of business processes and the fact that they are permanently exposed to numerous vulnerabilities, it becomes obvious to include business processes into security considerations. As business processes generate value and their unimpeded execution is vital for the success of enterprises, decision makers and security experts are tasked with revising methods to secure them against external or internal threats; legal requirements and the loss of value sustained after a successful attack result in the demand for appropriate security measures. Loss of value can be either of monetary nature (e.g. loss of profit due to the interruption of business activities) and/or intangible (e.g. loss of reputation). The following examples illustrate the severity of security breaches: In February 2000, a Denial of Service (DoS) attack caused access problems of Yahoo!'s website, costing an estimated half a million US Dollars in just three hours [Ked00]; in 2000, the worldwide economic impact of high profile incidents due to malicious code amounted to $17.1 billion, with 8.75 billion solely related to the infamous Love Bug virus [Com04]. The consequence is an ever increasing amount of money spent on improving security (from 1999 to 2000, the number of organizations spending more than $1 million annually on security nearly doubled, representing 12% of all organizations in 1999 and 23% in 2000 [Bis03]). But whether these expenses are spent optimally is often not determined, and more often than not security investments are either too low or high.

1.2. Problem Statement

A major problem with defining Secure Business Processes is the fact that security considerations are basically not integrated into business process development. This is the result of inappropriate (or even missing) security policies that almost completely neglect business processes. The cause is twofold: On the one hand, during development, security considerations were not included in process specifications innately, but ignored at all. The reason is that business process modeling (and specification) methodologies do not provide means for specifying security semantics at all, e.g. the Unified Modeling Language (UML) [Kob99] and the Architecture of Integrated Information Systems (ARIS) [Sch92] are two of the most common modeling languages for business processes, and both do not include any methods for modeling security-related entities. As a result, security extensions had to be added afterwards (cf. [Jür02], [RFMP06], [MC05], [zMR05]). On the other hand, security properties are mainly considered as 'technical' problems which have to be solved by dedicated security experts [Her99]. Process managers, not having enough security specific knowledge, are tasked to develop optimal business processes according to the business strategies without any thought about security. As a result, the security departments are often not integrated into the corporate core areas [NKB06] [Pfl97] [GK95], thus leading to a separated development of processes and security.

The main problem with security, however, is how to measure it. Recent approaches depend on the calculation of aggregated values such as the Annualized Loss Expectancy (ALE) [fip79] or Return on Investment (ROI) for evaluating security improving measures. But relying solely on a single value for measuring security is inappropriate, considering the multiple factors that may play a role: Obviously, as a result of a safeguarding procedure, business processes should be made resilient against security threats and security requirements need to be fulfilled. Since most companies have limited resources, the installed safeguards have to be cost effective as well. In short, different and often conflicting or mutually affecting factors (e.g. installation costs and running expenditures, manpower, installation time) as well as an unimpeded execution of the business process itself need to be considered. This multiobjective nature of the problem severely complicates the accurate measurement of security safeguards. Apart from respecting the different factors regarding security itself, stakeholders usually differ in their individual preferences of safeguards as well, thus making the agreement on an optimal safeguard portfolio even more difficult [NSW06].

Part of this measurement problem is the issue of ’How much (security) is enough’ [Soo00], as security does not directly generate business value and does not directly improve the net profit [NKB06]; investing in security can only prevent negative events or reduce related adverse effects. A compromised execution (or stopping) of business processes due to incidents such as viral attacks, data theft, or hardware failure may result in considerable negative effects. But those negative events are not guaranteed to occur, wherefore, facing no such incident, high investment in security could be seen as a waste of money. As a consequence, companies do not know if their often considerable investments into security are effective at all. Security measures are often implemented as a result of immediate needs and represent only punctual solutions without carefully weighing the benefits against the costs. This circumstance is further intensified by the fact that decision makers are often driven by fear when applying security measures [NKB06]. Another issue with ’how much’ is that, there is no way to protect a system against every conceivable or theoretical weakness with limited resources [Buz99]. Therefore, it is the aim to make the system as secure as necessary, but not securer [San03].

1.3. Research Questions and Aim of this Thesis

The stated problems can be formulated into the following research questions:

- How can the optimal combination of safeguards for a given business process be determined with respect to multiple objectives?
- Are multiobjective decision making techniques applicable for safeguard evaluation?
- Is it beneficial to combine multiobjective decision making and risk management methods to construct a holistic methodology for eliciting the needs for security and safeguards?
- How can risks be identified using business process models?

The goal of this thesis is to answer these questions by proposing an integrated framework for assessing the risks business processes are exposed to and for finding appropriate security controls, based on the work done in [NSW06], [Neu07], [NS07a], [NS07b], [NH07a], [NH07b], [NH07c], [NH07d], [NH08]. It is not the aim to develop another technical solution for countering specific threats, but to find a methodology for analyzing the need for security measures and for arranging the optimal safeguard portfolio.

1.4. Proposed Methodology

The proposed solution for the problems stated above is a model-supported, risk-based multiobjective decision making process (MR-MOD). It combines elements of multiple techniques into one integrated framework to address the different difficulties of security evaluation of processes and safeguard selection:

Process Models A (graphic) process model is used for eliciting security problems and requirements to account for the process-centered view of today's business activities. This includes the identification of process crucial assets and threats they are exposed to.

Quantitative Risk Assessment The quantitative risk assessment provides a structured process to evaluate the severity of harmful risks and appropriate risk mitigation strategies, based on the usual perception of risks as asset/vulnerability/threat-tuples.

Workshop By structuring the risk assessment process in a workshop environment, the methodology allows for multiple persons to participate and, thus, preferences and the knowledge of different stakeholders can be taken into account.

Multiobjective Decision Making A Pareto-based multiobjective decision making process ensures the consideration of the different properties of safeguards such as effectiveness and costs when determining the optimal portfolio.

The MR-MOD framework is divided into the following three distinctive phases:

Phase 1: Modeling and Identification The first phase serves as preparation phase for the risk assessment, providing input data for the following phase (assets, threats, vulnerabilities, safeguards).

Phase 2: Workshop-based Risk Assessment The next phase deals with the risk assessment of the pre-defined entities in a workshop process that is tasked with defining cost/benefit categories and assigning values to the entities.

Phase 3: Multiobjective Decision Making The final phase makes use of the information gathered in the preceding phases to calculate the optimal allocation of security safeguards.

1.5. Structure of the Thesis

The remainder of the thesis is organized as follows:

Chapter 2 provides fundamental background information including the historical background and benefits of business processes, the definition of security and explanation of security attributes, the categorization of different risk assessment approaches and explanation of risk-related terminology, and the description of multiobjective decision making and Pareto-dominance in particular.

Chapter 3 provides an overview of some methodologies found in literature that are related to information security, risk analysis and assessment, and multiobjective decision making, including the decision support technique AHP, the process-based information security elicitation methodology POSeM, and risk assessment approaches such as CRAMM and OCTAVE. In addition to a short description, some applications as well as pros and cons are given.

Chapter 4 introduces the main issue of this thesis, the MR-MOD framework. The three phases are explained, beginning with a short overview and required participants, followed by detailed descriptions of all sub-steps of each phase.

Chapter 5 presents the development of a software tool to support the MR-MOD framework, the MODStool application. At first, the basic requirements are specified, followed by a detailed explanation of all functions including screenshots, an overview of the technical architecture, and the description of the underlying data model.

Chapter 6 evaluates the feasibility of the MR-MOD methodology by means of a case study. All MR-MOD steps are demonstrated on an exemplary process model representing a typical insurance claim process.

Chapter 7 provides a comparison of MR-MOD with the two frameworks AHP and POSeM to evaluate the advantages and disadvantages of each methodology. To acquire comparable results, the same test scenario of chapter 6 is applied, adapted to the individual characteristics of the other methods.

Chapter 8 summarizes and reviews MR-MOD and discusses whether all research questions were answered.

2. Fundamentals

This chapter introduces several concepts used in this thesis including business process management and modeling, security, risk management, and multiobjective decision making.

2.1. Business Process Management

The definitions of the term Business Process found in literature are diverse. The Workflow Management Coalition (WfMC) defines business processes as

> A set of one or more linked procedures or activities which collectively realise a business objective or policy goal, normally within the context of an organisational structure defining functional roles and relationships. [WFM99]

Jacobson et al. describe a business process similarly as

> The set of internal activities performed to serve a customer. [JEJ94][1]

Ferstl and Sinz provide another definition for a business process:

> A transaction or a series of transactions between business objects. The subject of the transaction is the exchange of services and/or messages between objects. [FS93][2]

Snowdon and Worboys explain the following:

> A company uses its 'assets' (financial, intellectual, material) to add value to its 'inputs' in order to produce 'outputs' from which it can directly, or indirectly, increase its assets and make profits. This we may call the company 'process'. [SW94][2]

[1] In [LDL03].

[2] In [Röh03].

And finally, Röhrig defines a process in her PhD-thesis as

> an ordered sequence of activities, carried out to a specified end, executed by certain defined actors, that has clearly identified inputs and outputs. [Röh03]

Reflecting the diversity of definitions for business processes, there is a multitude of explanations for business process management (BPM) as well, beginning with the definition given by Weske et al.:

> Supporting business processes using methods, techniques, and software to design, enact, control, and analyze operational processes involving humans, organizations, applications, documents and other sources of information. [WvdAV04]

Elzinga et al. define business process management as

> a systematic, structured approach to analyze, improve, control, and manage processes with the aim of improving the quality of products and services. [EHLB95]

Röhrig provides another definition in her PhD-thesis for process management:

> Process management describes all activities concerning the handling of business processes, i.e. the definition and modelling of processes as well as the procedures regarding their execution. [Röh03]

Zairi explains BPM as

> A structured approach to analyse and continually improve fundamental activities such as manufacturing, marketing, communications and other major elements of a company's operations. [Zai97][3]

And Lee and Dale consider BPM as

> a customer-focused approach to the systematic management, measurement and improvement of all company processes through cross-functional teamwork and employee empowerment. [LD98]

[3] In [LD98].

2.1.1. Historical View

(Business) Processes play a major role in business companies today, but it took some time until the concept of business processes has been established. In the 1980s, American corporations had to face powerful international (mainly Japanese) competition and were forced to improve their productivity by lowering costs, lowering cycle times, and enhancing quality and services [Ham96]. They also analyzed their business functions and applied the latest technological advances, but all these measures did not result in the anticipated and hoped-for performance boost. Then the managers realized the problem: their solutions were suited for solving task problems, but not for process problems. This was where the companies' functional view began to change to a process-oriented view [HM99]. Although these processes were central to their business activity, managers were not aware of them and therefore never considered improving them. With the advent of process-oriented thinking and the introduction of process-oriented business improvement programs, American corporations could reform their business activities, which led to the revitalization of the American economy in the 1990s.

Changing to a process-oriented view resulted in the demand for structural modifications in management styles, personnel, measurements systems, and the like; in short: a process-centered organization. Along with process-centering came another aspect: the customer-centering, which means that the companies have to focus on the customers' wishes and they have to act accordingly.

Generally, the shift to a process-centered company includes four steps [Ham96]:

Identification and Naming of the Processes Obviously, the first step consists of the identification of the key processes that create value for the business company. But this has to be done diligently (e.g. a simple relabeling of existing functional units as processes is inappropriate), as the correct identification of the processes is the basis for any improvements.

Awareness of these Processes The second step ensures that everyone in the company is aware of the identified processes. This does not change their individual tasks but it changes their mind-sets and lets them get the big picture.

Process Measurement In the next step, the companies need to devise measurements to know how well the processes are performing. Some of these measurements need to be based on customers' needs, some on the companies' ones. These measures are important for future improvements.

Process Management In the past, the focus on processes began when improvements were made on whole processes instead of single tasks. However, in order to stay competitive, these improvements need to be made continuously, and companies have to manage their processes actively. Therefore, the final step is process management: Managing a business means managing its processes, this is why business process management is so important.

The evolution of BPM can be aggregated into three 'waves' [LPS05]:

Process Improvement (1970s-1980s) Until then, the focus lied on specific tasks and their improvement. In the 1960s, technology became a business driver, as new technological advances were rapidly introduced. The international competition got fiercer and, as a result, US companies had to change their business paradigm: the process-era began. The advances in technology led to production speeds that enabled 'Just in time' manufacturing. Improvements were enforced on the process level and not on the task level anymore. The growing use of computers led to better data gathering techniques (quantitative statistical software), which resulted in better controlling. Technology became a process driver.

Process Reengineering (1990s) In the 1990s, American corporations could revitalize themselves and their revenues rose. The focus shifted to total quality management and later to ISO compliance standards; 'best practices' were introduced. The steady growth of statistical analysis required new meaningful ways of data management; new technologies such as Enterprise Architecture, Enterprise Resource Planning (ERP), and Customer Relationship Management (CRM) emerged.

Business Process Management (2000+) The third wave began in the mid 1990s and is lasting up until now. Technology is no longer a process driver, but a process enabler. Customers are no longer seen as an aggregated market, but as individuals that demand customized solutions. Just-in-time manufacturing led to Just-in-time supply chains with networked organizations; business processes stretch over multiple disparate enterprises. The focus lies on a high accessibility of the 24X7 global business. New technologies include Enterprise Application Integration (EAI), Service Oriented Architecture (SOA), and Business Process Management Systems.

2.1.2. Benefits of BPM

The introduction of BPM has several benefits, some of them are [Han03]:

Cost Reduction Automation of business processes leads to reduced human resource demands, and a leverage of existing IT-resources reduces the demand for investments in new technology for improvements.

Quality Improvements and Error Reduction Real time and historical reports provided by a BPM system lead to quality improvements, and automated processes using electronic forms help reduce data-entry errors.

Visibility Gain A BPM system lets decision makers gain a valuable insight into the processes, providing reports on benchmarks, key performance indicators (KPI), and other related data.

Process Step Automation One of the fundamental benefits of BPM, the automation of business process steps, reduces the workload of human employees and reduces the handling time of complex transactions.

Satisfaction Improvements The faster handling of order issues and problems and the higher transaction execution speed combined with a lower number of errors result in a higher satisfaction of customers, employees, and business partners.

2.1.3. Workflow Management Systems and Enterprise Resource Planning

Some of the concepts related to BPM are Workflow Management Systems (WFMS) [BW95], [BvUzMR99] and Enterprise Resource Planning (ERP) [SH00]. Both WFMSs and ERP systems are solutions for improving business activities and managing business processes [CBS04], but they rely on different approaches.

As the WfMC defines workflows as "The automation of a business process, in whole or part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules" [WFM99], workflow management can be seen as a part of business process management [WvdAV04]. In fact, WFMSs provide a workflow model that reflects specific business process structures. The actual workflows represent already existing business processes that are executed automatically. During execution, workflows can access legacy systems, databases, and they interact with the user. The WfMC has published a reference model [WFM95] that distinguishes build-time functions (defining and modeling the workflow processes and its constituent activities) and run-time functions (managing the workflow processes in an operational environment and the sequencing of the individual activities, interacting with human users and IT application tools).

On the contrary, ERP systems are actually prefabricated applications that are developed by vendors for particular sectors of the industry. Companies acquire modules according to their needs and the 'workflow model' is embedded in these applications. Where workflows in WFMS are developed specifically to meet business processes, customization is accomplished in ERP systems by setting parameters; the more parameters, the more flexible the system is. ERP systems are characterized as data-centric configurable information systems which manage and integrate the information and services of departments throughout an entire enterprise. Table 2.1 summarizes the differences of WFMSs and ERP systems (adapted from [CBS04]).

Table 2.1.: WFMS vs. ERP

	WFMS	**ERP**
Domain Scope	Customized processes Domain independence	Embedded processes Domain specific
Technological Scope	Process-centric Supports workflows involving humans, IT applications and transactional workflows	Data-centric Transactional Processes
System Implementation	Acquired as ready systems; Code automatically generated Bottom-up approach	Based on pre-written 'off-the-shelf' components Top-down approach

2.1.4. Business Processes and Security

Given the importance of business processes and the fact that they are permanently exposed to numerous vulnerabilities, it becomes obvious to include business processes into security considerations. As business processes generate value and their unimpeded execution is vital for the success of enterprises, decision makers and security experts need to revise methods to secure them against external and internal threats. Consideration of legal requirements and the loss of value sustained after a successful attack result in the demand for appropriate security measures.

Process models can be the basis for a structured elicitation of security properties. Using models of actual business processes, a security analyst can devise what needs to be protected and where a system is vulnerable. Then appropriate methods for closing these security gaps can be selected. Including a security analysis of business processes can even be an additional step in Business Process Reengineering (BPR): While processes are permanently improved, companies can ensure that these processes are protected optimally at all times as well.

2.2. Security

Finding an appropriate description of security is a difficult task. A general definition of security is given by Abrams and Jajodia:

> Security is the quality or state of being protected from uncontrolled losses or effects. [AJ95][4]

Some other definitions can be found in the Internet Security Glossary:

> (1.) Measures taken to protect a system. (2.) The condition of a system that results from the establishment and maintenance of measures to protect the system. (3.) The condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss. [Shi00].

Landwehr claims that

> a computer is secure if it is free from worry and if it is safe from threats, and computer security is the discipline that helps free us from worrying about our computers. [Lan01]

One reason for the difficulty in finding an exact definition for security lies in the fact that there are multiple forms of security within a company, e.g. operations security, production security, personnel security or computer security [Fin00]. In this thesis, the focus lies on information security.

[4] In [Röh03].

2.2.1. Information Security

Restricting the term security to 'information security' does not considerably simplify the search for an appropriate definition, as several authors tried to find a suitable description [Bis03], [Lan01], [Pfl97], [And03]. Information security can be seen as

> The protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information. [IBM84][5]

In the context of this thesis, the above definition is applied and the mentioned information assets should be regarded as related to business processes.

Despite of the lack of a generally accepted definition of (information) security, it is seen by organizations as something "Having it is obviously good" [Bis03]. This is reflected by the large and ever increasing amount of investment into security architecture [Bri00]: From 1999 to 2000, the number of organizations spending more than $1 million annually on security nearly doubled (representing 12% of all organizations in 1999 and 23% in 2000). The share of companies spending between $500K to $1M increased from 7% to 12% and between $100K and $500K from 18% to 33%. At the other end of the scale, the numbers decreased: While the share of companies spending between $50K and $100K declined from 14% to 8%, the numbers dropped from 49% to 23% in the under $50K security budget category.

Considering security as an important issue, the main question is not 'how to do' but 'how much is enough' [Soo00]. 'How' can easily be answered, as there are numerous methods for increasing security (cf. figure 2.1 [VE03]). 'How much' is a more complicated issue, since finding the optimal 'amount' of security is a difficult task. The problem is twofold:

On the one hand, security does not directly generate business value; investing in security can only prevent negative events or reduce related adverse effects. A compromised execution (or stopping) of business processes due to negative incidents such as viral attacks, data theft, or hardware failure may be accompanied with considerable costs, either monetary (e.g. loss of profit as a result of stopping the process) or intangible (e.g. loss of reputation), or both. But those negative events are not guaranteed to occur, therefore, facing no such incident, high investment in security may be a waste of money.

On the other hand, there is no way to protect a system against every conceivable or theoretical weakness with limited resources [Buz99]. Therefore, the aim of security

[5] In [Fin00].

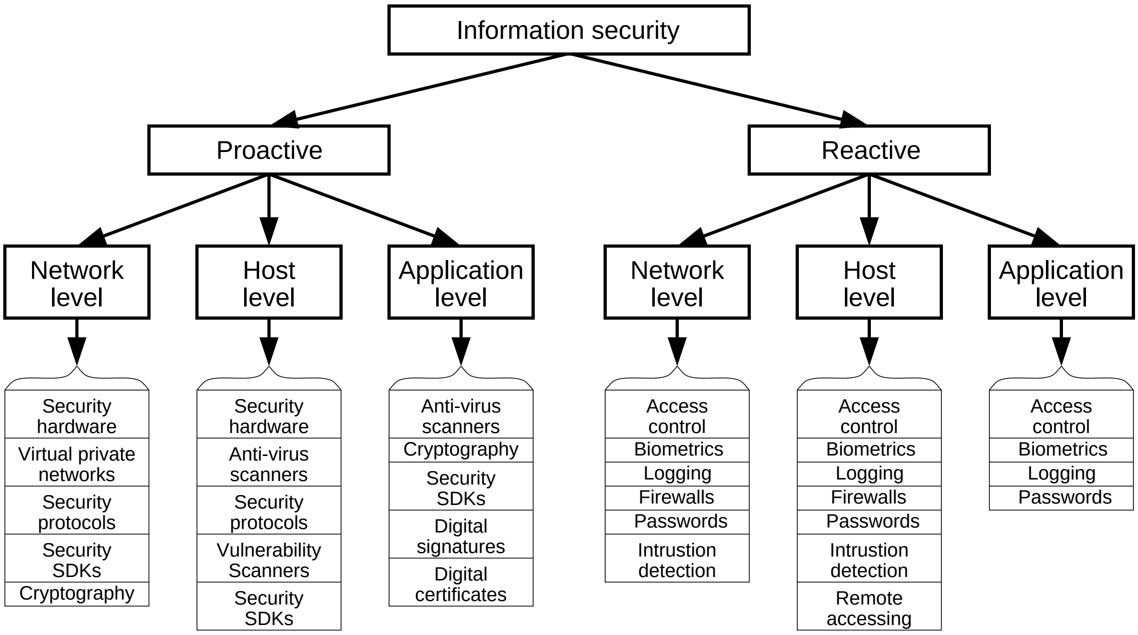


Figure 2.1.: Taxonomy of Information Security Technologies

management is to make the system as secure as necessary, but not securer [San03]. In order to determine the optimal investment, some kind of security measurement against security objectives needs to be applied.

According to Katzke, the following security objectives can be identified: Security requirements, best practices, security baselines, due diligence, and maturity models [Kat07]. A comparison along with examples is given in table 2.2 [Sad04].

Katzke also distinguishes between the following security measurement methods: direct testing, evaluation, assessment, accreditation, training/education/level of competence, and observation of system performance [Kat07] (cf. table 2.3 [Sad04]).

The approach taken in this thesis' proposal is a risk-based assessment against the due diligence objective (as the expertise of security experts, internal and external, is the basis for the security evaluation here).

Further aspects related to security are security policy and management. A security policy defines the extent of information to be protected and specifies high-level security requirements [Röh03]. The policies are often developed specifically for a particular organization: Consider a large commercial bank and a small company that provides a platform for publishing private web-content. These two organizations have vastly different security requirements and thus different security policies (although for organizations operating in the same domain the policies can be quite similar). Security Management

Table 2.2.: Security Objectives

Security objectives	**Application method**	**Expected result**	**Example**
Security requirements	Security actions are compared to requirement	Suggestions for improvements	Standards, Common Criteria (CC) Profiles
Best practices	Safe procedures for certain activity are given or determined	Instructions for secure procedures	Instructions for viruses, e-mail handling
Security baselines	Organization security inspection and assessment	Minimum set of security actions needed	Required access control
Due diligence	Security management based on expertise	Security level of own organization or business partner	Evaluation of security controls
Maturity models	Security practices are inspected and compared to the model	Explicit security level	SSE-CMM

deals with the implementation of the security policy [TS00] and all the steps of security measurement, and the selection of methods for improving the security can be seen as part of security management.

2.2.2. Dependability and Security Attributes

In literature, information security is described very often by the three aspects of Confidentiality, Integrity, and Availability (CIA) [BMG01], [Buz99], [Fin00], [GL02], [LV04], [Pfl97]. Recently Authentication and Non-Repudiation were added [Lan01], [Soo00], [Vid04]. Another related aspect is Reliability.

Avizienis et al. describe those kinds of aspects as dependability and security attributes [ALRL04]. Dependability is characterized as the ability of delivering justifiably trustworthy services or the ability to avoid unacceptable service failures. Dependability and security are interrelated by means of their attributes (cf. figure 2.2 [ALRL04]) and comprise of the following [ALRL04], [Lan01]:

Confidentiality refers to assuring that information is not disclosed without proper authorization.

Table 2.3.: Security Measurement Methods

Method of measurement	**How applied**	**Expected Result**	**Example**
Direct testing	System state is assessed by testing its qualities	Operational state of a system	Penetration testing
Evaluation	Security measures are compared with criteria	Baseline establishment, suggestions for improvements	Audits
Assessment	Security measures are assessed	Prioritized actions, suggestions for improvements	Risk analysis techniques
Accreditation	Security measures are assessed	Possible certificate, suggestions for improvements	ISO 9000 Series certificate
Training, education, level of competence	Personnel and organization knowledge is assessed and increased	Possible certificate, improvements in individual expertise	Conference, skill tests, meetings
Observation of system performance	System is monitored with technical tools	State or quantity of some technical feature in a certain moment or period	Intrusion detection, network load measurement

Integrity refers to assuring that information is not modified without proper authorization.

Availability refers to assuring that information is accessible to users when required.

Reliability refers to the continuity of correct services.

Safety refers to assuring that catastrophic consequences on the user and the environment do not occur.

Maintainability refers to the ability of services to undergo modifications and repairs.

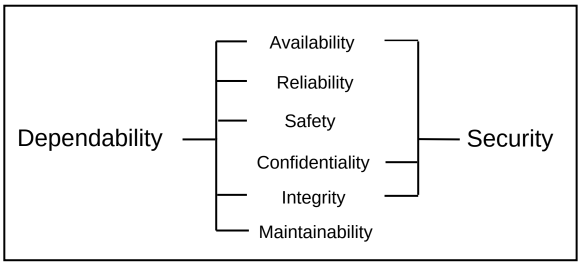


Figure 2.2.: Dependability and Security Attributes

Avizienis et al. have added threats to these attributes and means to attain these attributes to their taxonomy. The threats include [ALRL04]:

Failures are events where the delivered services deviate from correct services.

Errors are states of services that are deviated from correct ones.

Faults are adjudged or hypothesized causes of errors.

The means to attain the dependability and security means can be grouped into four categories:

Fault Prevention refers to preventing the occurrence or introduction of faults.

Fault Tolerance refers to avoiding service failures in the presence of faults.

Fault Removal refers to reducing the number and severity of faults.

Fault Forecasting refers to estimating the present number, the future incidence, and the likely consequences of faults.

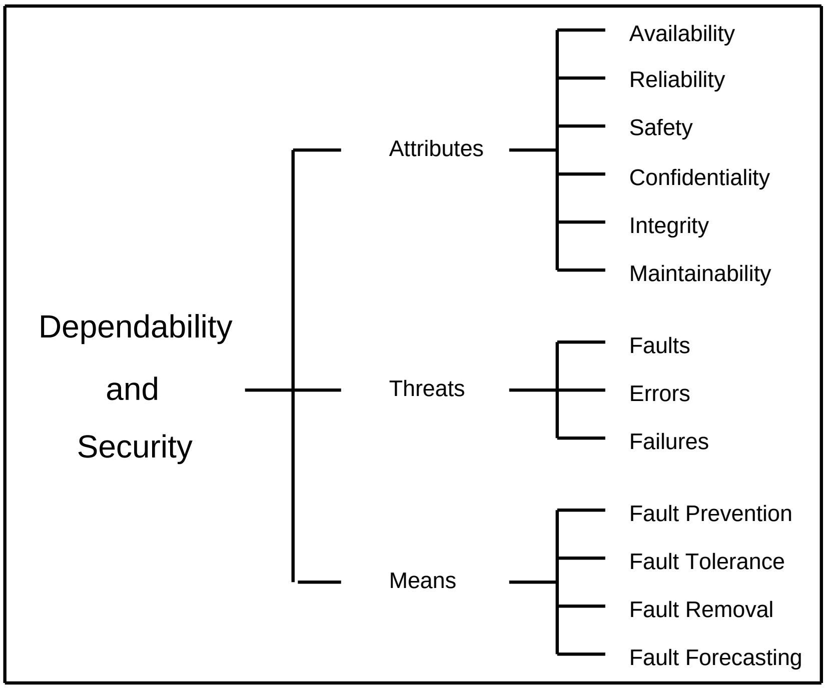


Figure 2.3.: Dependability and Security Tree

These concepts are summarized in a dependability and security tree (cf. figure 2.3 [ALRL04]). In the following, unless otherwise stated, security attributes or properties refer to the standard confidentiality, integrity, and availability.

2.3. Risk Management

A risk is generally defined as

> the potential, or probability, of an adverse event. [CFBZC02]

Galway describes risks in a similar manner:

> A risk is an event, which is
>
> - uncertain
> - has a negative impact on some endeavor. [Gal04]

Turban et al. are a bit more specific and define a risk as

> the likelihood that a threat materializes. [TMW96][6]

[6] In [Fin98].

The concept of risks may be applied to different areas, including everyday life, e.g. anybody that drives a car is exposed to the risk of having a car accident. In business terms, a risk is "the possibility of an event which would reduce the value of the business were it to occur" [BMG01]. When applying risks to information systems in a business environment, different kinds of risks can be identified, e.g. financial, technological, security, or information risks [SMS01]. In the context of this thesis, the relevant type of risk is (information) security risk that refers to security issues within business processes.

The process of handling risks is called risk management. In business context, risk management is described as

> the practice of using risk analysis to devise management strategies to reduce or ameliorate risk. [Gal04]

In conjunction with security, Caelli et al. define risk management as follows:

> Risk management has the aim to identify, measure and control uncertain events in order to minimize loss and optimize the return on the money invested for security purposes. [CLS89][7]

Related to (information) security risks of business processes, Peltier defines risk management as

> the process that allows business managers to balance operational and economic costs of protective measures and achieve gains in mission capability by protecting business processes that support the business objectives or mission of the enterprise. [Pel05]

Furthermore he describes risk management as the total process of identifying, controlling, and minimizing the impact of uncertain events and specifies four distinct steps:

Risk Analysis Technique to identify and assess factors that may jeopardize the success of a project or achieving a goal, to define preventive measures to reduce the probability of these factors from occurring, and to identify countermeasures to successfully deal with these constraints.

Risk Assessment Computation of the identified risks as a function of assets, threats, and vulnerabilities (cf. taxonomy).

[7] In [Fin98].

Risk Mitigation Process of implementing controls and safeguards to prevent identified risks from occurring, and/or the implementation of a means of recovery in case of risk realization.

Vulnerability Assessment and Controls Evaluation Examination of a critical infrastructure to determine the adequacy of present security measures, identify security deficiencies, evaluate alternatives, and verify the adequacy of these alternatives after implementation.

Apart from this specification, there is a wide range of deviating definitions for risk assessment and risk analysis, and there is no consent on the distinction of those two concepts among the different researchers: For example, the European Network and Information Security Agency (ENISA) specifies risk analysis as part of the risk assessment process (along with risk identification and risk evaluation) [eni06], while Galway, in turn, describes risk analysis as the "process of quantitatively or qualitatively assessing risks" [Gal04]. In this thesis, the terms risk assessment and risk analysis are interchangeable and include the identification and assessment of risks, as well as the identification of suitable security measures to deal with the risks (cf. figure 2.4 [eni06]). Generally, risks may be treated in four ways [Jon07]:

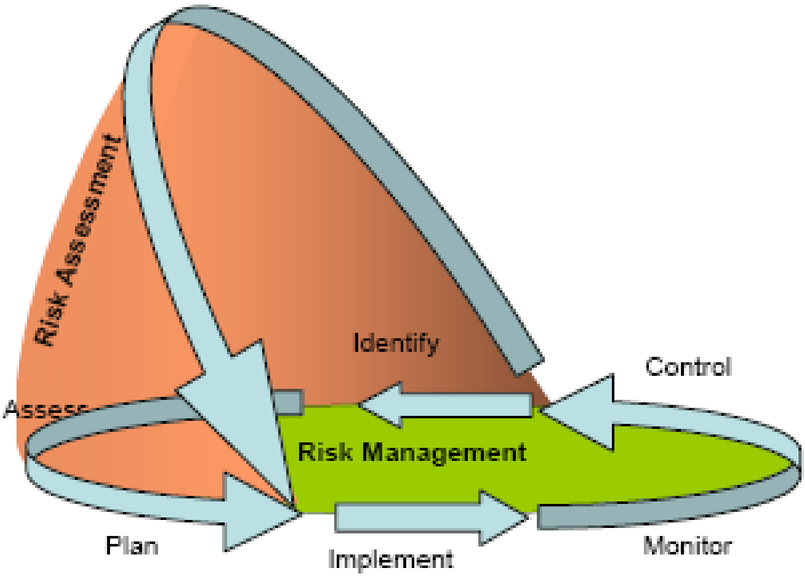


Figure 2.4.: Risk Assessment as Part of Risk Management

Risk Avoidance This normally entails not performing an activity that could carry a potential risk, which would limit the functionality of the system.

Risk Reduction or Mitigation This encompasses methods that are taken to reduce the severity of the impact of an incident or its probability of occurrence. Particular interest lies in the balance between the costs of risk mitigation measures and their benefits.

Risk Acceptance This is the approach where the impact that results from an incident is accepted when it occurs. Often, negligible risks or risks whose mitigation costs would be greater than potential losses are generally accepted.

Risk Transfer The final method of risk treatment is transferring the risks to another party, typically by either contract or insurance.

Risk analysis is a capable method to manage information security and is the foundation of many security management frameworks, e.g. the CCTA Risk Analysis and Management Method (CRAMM), the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), or the Facilitated Risk Analysis and Assessment Process (FRAAPS). However, the application of risk analysis is not restricted to information security but also successfully applied to assess other types of risks. Some examples of other domains are software development [GC04], geotechnical engineering [HLR00], business process reengineering [CFBZC02], or even maritime risk assessment [MH07].

2.3.1. Terminology

The following section contains explanations of risk-related entities.

Asset

Assets are entities of a system that have a certain amount of value and play a major role for the business activities, thus needing protection, or in other words, "whatever you're trying to protect" [Ham02]. Assets may be categorized into the following two [Pel05]:

Physical Physical assets are tangible items that can be seen, including computer servers or production machinery.

Logical Logical assets refer to the intangible intellectual property of the enterprise, including customer data or other information.

The British BS7799 provides another, more refine, classification of assets [BSI99][8]:

[8] In [CKL$^+$05].

Information Assets Data bases, study and training material, management plans

Documents Contracts, guidelines, important business documents

Software Assets Application software, development tools, utilities

Physical Assets Computer equipment, data storage media, production machinery

Personnel Assets Individuals, customers, subscribers

Image and Reputation of a Company Influences market position, sales

Services Computer and communication services, light, electric power

Threat

A threat is the "potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability" [SGF02]. Without an exploitable vulnerability, threats pose no risk. Generally, threats can be categorized into three major threat sources [Pel05], [SGF02]:

Natural Threats Natural threats include tornadoes, floods, fire, or other events caused by Mother Nature.

Human Threats Human threats are caused or enabled by human beings and can be further separated into unintentional acts (such as input errors due to mistyped characters) and deliberate actions (virus uploads, network attacks, unauthorized intrusion). Statistically, human errors and omissions are the threats causing the largest losses.

Environmental Threats Environmental threats include incidents such as power failure, liquid leakage, and hardware failure because of wear.

Human deliberate attacks may further be categorized according to their techniques [FNES03]:

Physical Physical means can be used to gain access to restricted areas, e.g. computer room.

Personnel Personnel penetration techniques deal with subverting personnel authorizing some degree of access and privilege regarding a system (social engineering).

Hardware Attacks against hardware may be undertaken to use this hardware to subvert or deny the use of the system. Hardware attacks can be physical attacks, bug implantation, or attacks against the supporting utilities.

Software Attacks against software can range from discreet alterations, which are subtly imposed for the purpose of compromising the system, to more obvious abuse resulting in the destruction of data or other important system features.

Procedural A lack or inadequacy of controls may be exploited by users to penetrate a system, e.g. unauthorized personnel picking up classified data.

Vulnerability

A vulnerability is "a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy" [SGF02]. Vulnerabilities may be separated into the following types [Vid04]:

Physical Attackers may exploit the physical weaknesses of systems (e.g. missing physical locks) to gain access to restricted areas and tamper with or steal assets such as hardware, discs, etc.

Natural Some assets are especially vulnerable to certain natural and environmental threats. A typical example may be the physical proximity of assets to a large heat source or water pipe.

Hardware/Software Hardware and software may exhibit certain vulnerabilities that can be utilized for a system penetration, e.g. a not updated operating system is vulnerable to all sorts of intrusion attacks.

Media Improper handling of discs and other storage media may result in partial data loss or complete destruction of the media, or may be stolen.

Communication In a network environment, computers need to communicate with each other. Without proper mechanisms, these messages may be intercepted, leading to data leakage.

Human People are often targets of social engineering and lack of training / experience may result in all sorts of problems. Other factors may be greed, revenge, and the like of unsatisfied employees that may intend to harm the system.

The resemblance of these categories with the threat types is not coincidental, as threats exploit vulnerabilities and therefore are closely tied to them.

Risk

Risks are composed of assets, vulnerabilities, and threats and represent the combination of a threat exploiting some vulnerability that could cause harm to some asset. Formally, risks can be represented by an asset/vulnerability/threat-tuple.

$$Risk = Asset \circ Vulnerability \circ Threat \tag{2.1}$$

Smith states the following interrelation of assets, vulnerabilities, and threats:

> Risk in any context is the sum of threats (those events that cause harm), vulnerabilities (the openness of an enterprise to the threats) and asset value (the worth of the asset in danger). Increase any of these factors and the risk increases; decrease any and the risk decreases. [Smi93][9]

Thus he implicates an additive composition of risks:

$$Risk = Asset + Vulnerability + Threat \tag{2.2}$$

Apart from the representation by an a/v/t-tuple, risks may be defined in other ways, e.g. as the "product of probability of an occurring a given number of times per year (P) and the cost (or loss) (C) attributed to such exposure" [Cou77]:

$$R = P \times C \tag{2.3}$$

This representation utilizes two attributes commonly associated with risks, namely impact and probability [JMV+07]:

Impact Impact refers to the consequences of the risk-realization related to the system, e.g. the revenue losses due to a business process disruption or the replacement costs of damaged hardware.

Probability Probability refers to the relative chance that this negative event will occur. It may be expressed quantitatively in terms of the Annual Rate of Occurrence (ARO) or by a percentage, or qualitatively in scales (high, medium, low).

[9] In [Fin98].

Impact and probability are implicitly included in the former risk representation too, as the probability of a risk realizing is expressed by the probability of a threat successfully exploiting a certain vulnerability; the impact is given by the value of the asset. Thus, the latter representation is basically the same as the former, using a different terminology.

Safeguard

Safeguards are all kinds of measures that can be put in place to "possibly eliminate the risk, or at least reduce the risk to an acceptable level" [Pel05]. Note that these include not only technical solutions (such as firewalls), but nontechnical ones as well (management and operational controls such as policy introductions or employee training sessions). Safeguards, or security controls, tackle risks by reducing their probability of occurrence and/or by reducing their negative impact.

Safeguards can be further subdivided into the following categories [Pel05]:

Avoidance Controls Proactive safeguards that attempt to minimize the risk of accidental or intentional intrusions, e.g. encryption methods or security policies.

Assurance controls Tools and strategies employed to ensure the ongoing effectiveness of the existing controls and safeguards, e.g. penetration testing or perimeter scans.

Detection Controls Techniques and programs used to ensure early detection, interception, and response for security breaches, e.g. intrusion detection tools.

Recovery Controls Planning and response services to rapidly restore a secure environment and investigate the source of the breaches, e.g. investigation tools.

2.3.2. Risk Assessment Approaches

There is a multitude of different risk assessment methods which can basically be categorized into the following two [Vid04], [Pel05], [RSC91], [SH03]:

Quantitative Approach Quantitative risk assessment uses a mathematical approach and involves the measurement of the amount of damage done to an asset as a result of a compromise. This is a time consuming and expensive activity which requires hard facts and numbers that are often not easily accessible. The solutions of this approach are based on probability. Some quantitative techniques are:

- The Annualized Loss Expectancy (ALE) [Pic89] method is a widely used method to analyze risks. It analyzes the assets, possible threats, and vulnerabilities and expresses the risks as a function of probability and impact. The formula is
$$\mathit{Total\ IT\ Risk\ Exposure} = \sum_{i=1}^{n}(V_i \times EL_i), \tag{2.4}$$
where $V_i = \mathit{vulnerability}$ (probability of occurrence per year) and $EL_i = \mathit{expected\,loss}$ (expected loss of i-th threat/vulnerability pair).

- The Livermore Risk Analysis Methodology (LRAM) [Gua87] operates similarly to ALE, but it expresses individual risk elements involving the occurrence of a single event loss, in contrast to producing a total risk measure:
$$R(RE_i) = MPL(C_i) \times PCF(PMC_i) \times EF(T_i), \tag{2.5}$$
where $R(RE_i)$ is the annualized measure of risk of the i-th risk element, $MPL(C_i)$ the maximum potential loss from unmitigated consequences of a threat to an asset, $PCF(PMC_i)$ the probability of a control failure of a set of (preventive and mitigative) controls, and $EF(T_i)$ the expected frequency of a threat (in terms of annual probability).

- The Courtney method [Pic89] is another ALE modification with adopted scales of magnitude:
$$\mathit{Total\ IT\ Exposure} = \frac{10^{(p+v-3)}}{3}, \tag{2.6}$$
where p is an integer representing orders of magnitude of estimated frequencies of a loss, and v an integer representing orders of magnitude of impact of an asset's loss.

Qualitative Approach Qualitative risk assessment is considered far simpler than the quantitative approach, as no probabilities are required and only estimated potential loss is used. Qualitative techniques express risks in terms of descriptive variables (such as Likert scales from 1-5), instead of precise values and discrete events, thus not needing precise information that is often unobtainable. Among others, qualitative techniques include the following:

- Scenario Analysis [NS87] is a method where various scenarios are developed that describe how assets might be subject to loss due to threats. These scenarios are ranked according to their relative importance and identify the weaknesses of a system. As an excellent communication method, risks can be visualized by graphical representations of scenarios, which are especially useful in identifying vulnerabilities to intentional threats.

- Fuzzy Metrics [NS87] simply utilize natural language for expressing asset, threat, and security mechanism attributes. The fuzzy descriptors might be high, medium, and low, e.g. assets may be of high, medium, or low value and threat probabilities may be high, medium, or low. Exact numbers can be assigned to these scales as well, e.g. medium probability is defined between 0.3 and 0.7, or low asset value is specified as everything below $10000.

- Questionnaires [NS87] include predefined questions that are usually segregated into different functional areas and are often publicly available. Questionnaires are beneficial in that they address typical weaknesses of systems, but they are also quite generic and do not consider the particularities of different systems. They do not consider the probabilities and magnitudes of potential losses.

Quantitative and qualitative methods do not dominate each other, as both types pose different advantages and disadvantages. The quantitative approach often provides more accurate data and a better foundation for deciding on appropriate safeguards, but only if required quantitative input data is available. If not, the qualitative approach plays out its strengths. A summary of the strengths and weaknesses of both qualitative and quantitative methods is given in table 2.4 (adapted from [Pel05], [SH03]).

Apart from quantitative and qualitative risk assessment approaches, two more minor categories can be identified [Vid04]:

Knowledge-based Approach Knowledge-based risk assessment involves reusing typical 'best practices', which was extensively done in the old years of computers where the numbers of assets and threats were easily manageable. Questionnaires (see above) can be regarded as a knowledge-based method as well.

Model-based Approach A model-based risk assessment uses object-oriented modeling methods to describe and analyze risks. A typical example of this type of risk analysis is the CORAS framework [LHSS03], a methodology that provides a UML-based framework for the graphical modeling of risks and their analysis.

Table 2.4.: Pros and Cons of Qualitative and Quantitative Risk Assessment Methods

	Quantitative Methods	**Qualitative Methods**
+	Applicability to all assets	Simple risk calculation
	Mathematical foundation	No necessity to determine monetary value of assets
	Great effort is put into asset value definition	Less time consuming
	Support to cost-benefit decision	No necessity to quantify threat frequency
	Results can be expressed in management-specific language	Easier to involve non-security and non-technical staff
-	Calculations are complex	Coarse granularity
	Time Consuming	Inability of cost-benefit decision
	Large amount of preliminary work	Very subjective results
	Difficult to change directions	Limited effort is required to develop monetary value for targeted assets
	Inappropriateness of monetary asset values and general statistics	

2.4. Multiobjective Decision Making

Multicriteria Decision Making (MCDM) is a scientific area that covers the decision process considering multiple, often mutually conflicting, factors. The classic approaches of dealing with multiple criteria, like converting the multiple objectives into a single objective by aggregation to a single scalar value, are often inappropriate. MCDM methods particularly address these multiple factors and provide means for an efficient decision making process.

2.4.1. Multiobjective Decision Making vs. Multiattribute Decision Making

In literature, MCDM methods are roughly categorized into two types [SY98][10]:

Multiobjective Decision Making (MODM) MODM refers to optimization problems. The search for efficient solutions is based on the optimization (minimization and maximization) of the different objectives and the best solutions are selected from

[10] In [Li07].

a large set of alternatives. Usually, the solution space is continuous (but not restricted to).

Multiattribute Decision Making (MADM) MADM refers to selection problems. The best solution is determined from a finite and usually small (pre-selected) set of alternatives. The selection is based on evaluating the objectives and their preference information.

The following section provides a formal description of Pareto-based evaluation, which uses the concept of dominance. "A solution x is said to be non-inferior or non-dominated if there is no other solution that is better than x in all the criteria" [SBP04].

2.4.2. Pareto-based Multiobjective Optimization

The general Multiobjective Optimization (MOO) problem can be written as [Jas04], [SBP04], [ZLB04]

$$\begin{aligned} &optimize\ \{f_1(x) = z_1, f_2(x) = z_2, \ldots, f_j(x) = z_j\} \\ &s.t. \quad x \in X \quad and \quad z \in Z \end{aligned} \tag{2.7}$$

whereas optimize can be either maximize or minimize, depending on whether the problem is a maximization or minimization problem. The solution vector $x = [x_1, x_2, \ldots, x_I]$ is the vector of decision variables and X the set of feasible solutions, also called the solution space. For discrete variables, the MOO problem is called a Multiple Objective Discrete Optimization (MODO) problem, Multiple Objective Combinatorial Optimization (MOCO) being a particular class of these where $x \in [0, 1]$. The so called point $z^x = [z_1^x, z_2^x, \ldots, z_J^x] = f(x)$ represents the image of a solution x in the J-objective space Z, such that $z_j^x = f_j(x)$ for $j = 1, \ldots, J$.

Using the concept of Pareto-dominance, (in case of maximization) point z^1 strictly dominates z^2 if $z_j^1 > z_j^2$ for $j = 1, \ldots, J$; point z^1 (loosely) dominates z^2 if $z_j^1 \geq z_j^2$ for $j = 1, \ldots, J$ and $z_j^1 > z_j^2$ for at least one; if neither points dominate (strictly or loosely), they are called incomparable.

Now, a solution $x \in X$ is called Pareto-optimal (efficient) if there is no $x' \in X$ that dominates x. The image $z \in Z$ of a Pareto-optimal solution is called non-dominated or non-inferior. The set of optimal solutions $X* \subseteq X$ represents the Pareto (-optimal) set, whereas its image $Y* \subseteq Y$ in the objective space represents the non-dominated set or Pareto front. A Pareto front approximation is a set A of points, and their corresponding solutions are such that there exist no $z^1, z^2 \in A$ that z^1 dominates z^2. That means the set A is totally composed of mutually non-dominated points.

Pareto optimization deals with finding the Pareto-optimal front or a set that represents a good approximation to that front. This technique is quite successful because there is no single-best solution (there are several solutions that represent different 'tradeoffs' between the objectives) and it is rather difficult to find a preferable ordering of the criteria.

3. An Overview of Concepts related to Information Security Safeguard Selection

Dealing with the information security of organizations and their business processes involves considering concepts of multiple research areas, such as dealing with threats and risks, considering security-related aspects of processes, and decision support for selecting suitable security safeguards.

The following chapter introduces some frameworks from the research areas mentioned above.

3.1. Analytic Hierarchy Process - AHP

The Analytic Hierarchy Process (AHP) developed by Saaty [Saa80], [Saa90], [Saa94] is a tool for solving multicriteria decision making problems and is based on the principles of hierarchy, pairwise comparison, and weight synthesizing for prioritizing criteria and the evaluation of alternatives. Specifically, the process consists of the following steps:

1. **Structuring a Hierarchy** At first, the whole decision problem is decomposed and structured in a hierarchy. Beginning with the overall goal of the process, criteria and sub-criteria are defined, and then alternatives to be evaluated are added. The result is a hierarchy tree with the overall objective as the root node, followed by criteria and sub-criteria, and the alternatives on the lowest level. Sub-criteria have to be defined in a way that elements of the same level are to be comparable to each other regarding their parent element. Note that there is no need for a complete tree, i.e. that each branch of the tree has to have an element on each specified level.

2. **Prioritizing the Criteria** The next step is to prioritize the criteria by comparing

them with each other pairwise (on the same level) according to their relative importance with respect to their parent element and assigning that comparison an intensity level between 1 and 9. Table 3.1 summarizes the possible intensity levels (adapted from [Saa80]).

Table 3.1.: Intensity Levels of AHP

Intensity of Importance	**Definition**	**Explanation**
1	Equal importance	Two elements contribute equally to the objective
3	Moderate importance	Experience and judgment slightly favor one element over another
5	Strong importance	Experience and judgment strongly favor one element over another
7	Very strong or demonstrated importance	An element is favored very strongly over another; its dominance demonstrated in practice
9	Extreme importance	The evidence favoring one element over another is of highest possible order of affirmation
2,4,6,8	For compromise between the above values	Sometimes one needs to interpolate a compromise numerically because there is no good word to describe it

The pairwise comparison is done by constructing a nxn-matrix (for each parent criterion with n child sub-criteria) and inserting the intensity level for each comparison, in total n(n-1)/2 comparisons because of reciprocals[1]. If all comparison matrices are constructed, weights are assigned to each criterion by calculating the maximum eigenvalue and eigenvector of each matrix[2]. Each matrix is also checked for consistency, expressed by the Consistency Ratio (CR) that refers to inconsistencies in the judgments, e.g. if element A is considered two times more important than B and element B three times more important than C, transitivity implies that element A is six times more important than C. The judgments do not need to be perfectly consistent, but the CR should reach sufficiently low values. Otherwise, the judgments should be reconsidered.

3. **Evaluating the Alternatives** When all (sub-)criteria are assigned weights, the al-

[1] E.g. element A is strongly more important than element B with respect to parent element X, inserting a value of 3 in the A/B cell and the reciprocal value of 1/3 in the B/A cell.

[2] For more information refer to [Saa80].

ternatives are evaluated by the same pairwise comparison technique and assigned weights with respect to each low-level criterion. For numerous alternatives, this can lead to a very large number of comparisons (for nine alternatives, 36 single comparisons for each low-level criterion). Therefore, apart from direct comparison, the Ratings method may be used where all alternatives are assigned intensity levels with respect to each criterion, but independently from other alternatives[3].

4. **Calculating the Global Priorities** Finally, the global priorities of each criterion can be determined by weighting the local priorities by the global priorities of the parent criteria (which in turn are obtained by weighting their local with the global priorities of their parent criteria). Then, the global priorities of the alternatives can be calculated by weighting their priorities with the global ones of each sub-criterion and adding them. Generally, for synthesizing the local priorities of alternatives, two modes can be used: distributive and ideal. In the distributive mode, the individual weights of alternative with respect to a sub-criterion sum up to one. This is used when alternatives are dependent on each other. In the ideal mode however, all weights are divided by the value of the highest rated alternative (still for each sub-criterion) resulting in the highest ranked alternative as the ideal one for the particular criterion. This is done for obtaining the single best alternative regardless of the others. The result is a ranking of all alternatives, regarding their importance for each criterion and their weighting as well.

The relative simplicity of the AHP makes it the perfect candidate to be used in a wide range of application areas. The decomposition of an otherwise complicated decision situation and the focus on the pairwise comparison allow the decision makers to concentrate on two elements only, which considerably simplifies the decision making process. But AHP also suffers from some substantial disadvantages: For one thing, a complex decision problem with many criteria and alternatives requires a very large number of comparisons, which can quickly become unmanageable. For another thing, there is a phenomenon called rank reversal. Rank reversal may occur with AHP when a new alternative is added to the decision problem. In that case, priorities are added in the matrices for this new alternative and the former ranking of the other alternatives may change, e.g. alternative A is specified as being better than B, but adding an alternative C and recalculating the priorities may result in A being inferior to B[4]. This problem is well known and discussed in literature, e.g. [BG83], [Dye90], [Hol90].

[3] Saaty advocates the ratings method for 9 or more alternatives [Saa80].

[4] Example given in [Saa94].

Nevertheless, AHP represents a popular and widespread method for all kinds of selection, evaluation, and decision making applications in different fields (such as engineering, finance, and politics), and many papers have been published on its use as a standalone decision making tool [VK06], as well as integrated with other methods (e.g. mathematical programming) [Ho07]. For this thesis, the domain of information security is of particular interest:

Bodin et al. [BGL05] use the AHP for determining the best alternative out of three proposals from reputable companies to improve the information security situation of a manufacturing organization. They assume a fixed budget ($1 Mio.) for security investments and define confidentiality, data integrity, and availability as criteria (authentication, non-repudiation, and accessibility as sub-criteria for availability). They use the ratings mode for evaluating the alternatives, and six intensity levels from moderately high to exceptionally high are defined for each (sub-)criterion as end nodes; their weights are determined by pairwise comparison. Then, these weights are assigned to the alternatives according to their intensity rank. To substantiate the results, the whole process is repeated with additional proposals (alternatives) from the three companies with a budget of $1.3 Mio. The Chief Information Security Officer then makes his final decision based on the proposals' performance/cost ratio and incremental performance/cost ratio.

Suh and Han [SH03] integrate AHP with risk analysis techniques to develop a risk analysis methodology based on a business model. In this proposal, AHP is used for determining the relative necessity and importance of business functions that are broken down from the overall business model. The pairwise comparisons are conducted to calculate the local priorities of sub-functions with respect to their parent functions, and their global priorities represent the proportion of the organization's objectives that are accomplished by the sub-functions (the highest-level business functions are compared with the organization's pre-defined objectives). Then, the risk analysis process is conducted: Assets are identified and assigned to the business functions, resulting in the relative necessity of assets. The next step includes a threat and vulnerability assessment resulting in the determination of risk probability. Finally, an annualized loss expectancy (ALE) calculation is conducted to assess the overall loss due to business stopping.

Another combination of AHP with information security-related risks is presented by Guan et al. [GLWH03]. In this proposal, AHP techniques are used for assigning weights to criteria of the security risk evaluation and to determine the likelihood of risks. The impact analysis is conducted in a fuzzy environment and together with the likelihood

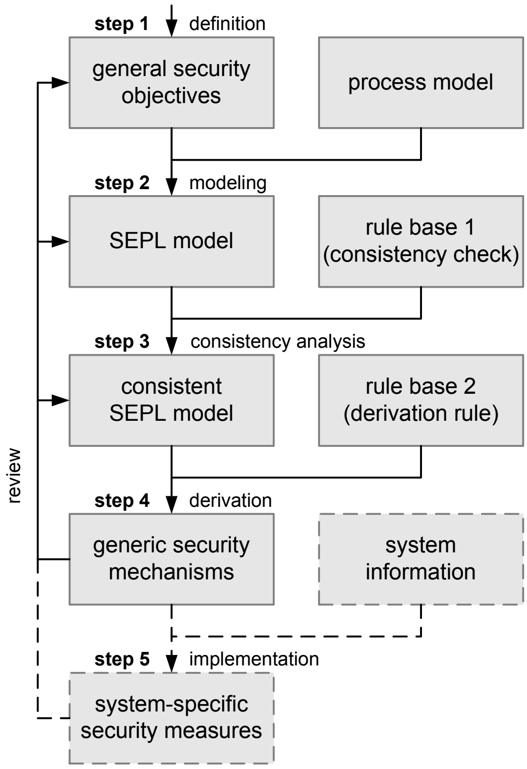


Figure 3.1.: POSeM Overview

values, the fuzzy risk values are calculated, represented by the Best Non-fuzzy Performance (BNP) value.

3.2. Process-Oriented Security Models - POSeM

The Process-Oriented Security Model (POSeM) framework developed at the University of Zürich by Röhrig [Röh03], [Röh02], [RK04] is a methodology to define security requirements and to derive security measures by using process models as the basis for the analysis. In this proposal, the four security objectives confidentiality, integrity, availability, and accountability are used to measure the security levels of each process component (actor, artifact, activity), and suitable security measures are derived via rule bases.

The POSeM approach consists of five steps (fig. 3.1 [Röh03]):

1. **Definition of General Security Objectives** At first, the general security objectives are defined in the form of a document that represents the overall security policy. This includes the definition of actor, artifact, and activity (called participant, data,

and activity in the POSeM framework) classes and addressing all four security objectives, as well as examining whether the security objectives conflict with the objectives of the business process itself. A possible candidate for a data class is 'Data to be published', having no confidentiality requirements at all, but higher availability, integrity, and accountability requirements. These classes are the basis for the SEPL model constructed in the next step.

2. **SEPL Model** In the next step, all components of the business process of interest are identified and given values for their security objective levels. By assigning all participants, data artifacts, and activities to one of the previously defined classes, they inherit their security levels that are later used for evaluation. Thereby the components are described in the so called Security Enhanced Process Language (SEPL), a modification of the Workflow Process Definition Language [WFM98]: Actors are called Participants and can be either Human or System, artifacts are labeled as Data and can be Data or Tangible (e.g. written letters), and activities (also called Activities in SEPL) can be a Transfer, Storage, or Manual task (these type markings are optional). Additionally, all components are assigned one of the following security (data and activities) or clearance (participants) levels for each security objective: None(0), Low(1), Medium(2), High(3), or Very High(4).

3. **Consistency Analysis** When the SEPL model of the business process is complete, it is checked for consistency with the rule base RB1. A consistency check usually involves testing the security levels of participant, data, and activity triplets, i.e. whether a certain participant assigned to a certain activity has a clearance level sufficiently high to carry out the activity on a certain piece of data. Inconsistencies can be removed by either altering the triple (e.g. reassigning another participant with a higher clearance level) or modifying the security levels of components (e.g. raising the clearance level of the same participant to meet the security level requirements of data and activity). The rules in the rule base are one of the following types: simple level rules ('greater or equal' relationship of security and clearance levels), separation of duty rules (definition of tasks that must not be performed by the same person), or composed rules (complex rules composed with logical relations). For this task, the Security Consistency Rule Language (SCRL) was developed.

4. **Derivation of Generic Security Measures** Using the consistent SEPL model generated in the previous stage, appropriate security measures can now be derived

with another set of rules, the rule base RB2. This rule base is implemented with the Security Measures Description Language (SMDL) where each safeguard is described, and their security objective levels are defined (only those, that are addressed by the safeguard), along with any Obsoletes (listing other security measures that become obsolete, when this particular safeguard is being implemented) and Depends_on (any safeguards that this particular one is dependent on) statements. The rules can be inserted into a derivation matrix showing all safeguards and their security levels, e.g. safeguard A with a confidentiality value of 2H for participants, 2 for data, and 2M for activities represents a safeguard that is suitable for human participants with the conf. clearance level of medium, data with conf. security level of medium, and manual activities, also with a conf. security level of medium. Using modules for different types of safeguards facilitates the definition of component types the measures are suitable for.

5. **Implementation Phase (Optional)** The final but not integral part of the POSeM framework and thus optional step is the implementation step where the list of generic security measures is further refined with system information to actual security safeguards. This includes the creation of specific instructions for the implementation of the safeguards.

After step 3, 4, and 5, a review should be conducted to check whether the outcomes of the individual steps are still in accordance with the main objectives defined in the first stage.

Röhrig has tested POSeM in two scenarios [Röh03]: The first scenario includes the development and management of documents to be published on a company website using a content management system where writer, editor, certifier, translator, and publishing daemon are the participants, the document in its different stages the main piece of data, and the tasks related to the document the main activities. Special attention lies in the fact that the security levels of the document to be published changes during its development stages. The focus of this scenario lies on integrity and accountability. The second scenario represents a part of a typical health reimbursement process in Germany where the reimbursement claims are collected, sorted, and sent by regular mail. Here, the focus lies on the confidentiality of claims and patient data.

The strengths of the POSeM approach lie in the usage of business process models as the basis for the security evaluation and the definition of organization specific rule sets for the consistency checks and safeguard derivation. Using process models seems to be a logical step in the process-centered world of today. As processes are continually improved (or completely restructured with BPR techniques), the security situation can also be evaluated and continually improved. Relying on the well established CIA properties also enhances the insight into security-related matters of processes, especially by assigning them to the individual process components (participant, data, activity). By defining organization-specific rules, the particularities of the organization and its main processes can be taken into consideration, thus reaching a high level of adaptability of the POSeM process. These rules can be specified once and stored for further uses, which significantly reduces the amount of time needed for the evaluation. And the formal description methods of SPEL, SMDL, and SCRL allow a possible high degree of automation, thus further reducing the workload. Another important fact is that there is no requirement of quantitative data like in another popular method for security evaluation, namely quantitative risk assessment, data which is often lacking.

But POSeM also possesses some weaknesses: As emphasized by Röhrig, this framework is mainly intended to elicit the requirements for safeguards, but not to decide which specific safeguards to choose. As a matter of fact, it is not suited as a standalone decision making method. The outcome of the evaluation is solely a list that is suitable for implementing the required security levels of the process components. This is underpinned by the fact that the economical factors of safeguards, namely their costs in monetary or time units, are completely neglected and only the technical aspect of security measures are evaluated. Furthermore, POSeM totally ignores any specific negative factors influencing business processes such as threats and vulnerabilities, which are integral parts of risk assessment practices. No harmful events such as a viral infection of the information system are considered and therefore no safeguards can be defined to counter that specific problem, which can be a major disadvantage of a framework that is specifically designed to be a security evaluation process.

3.3. Modeling Security Semantics of Business Processes - $MoSS_{BP}$

The framework for Modeling Security Semantics of Business Processes $MoSS_{BP}$ developed by Herrmann and Herrmann [HH06] is an approach aimed at eliciting and modeling security requirements of business processes and their components. It is designed to provide domain experts with a method to evaluate and model security-related properties of processes and derive security measures without the extensive help of a security expert. The framework relies on five different perspectives in order to produce an integrated, consistent, and complete view of the processes and their security requirements, represented by UML diagrams [HP98]: informational perspective (UML class diagrams for information entities and their structure), functional perspective (UML activity diagrams for activities and data flow between them), dynamic perspective (UML state chart diagrams for states and transitions of information entities), organizational perspective (UML class diagrams for actors), and finally business process perspective (UML swim lanes to integrate the other perspectives).

The $MoSS_{BP}$ architecture is organized into four abstraction layers containing repositories of reference models and building blocks to be consulted for implementing security requirements:

Layer 4 Contains high-level graphic concepts of typical business process elements and security requirements. UML diagrams for all perspectives are modeled by applying and adapting those concepts.

Layer 3 Contains reference models and case studies of sub-processes describing how to enforce security requirements. These include basic security elements and activities that are represented by UML models as well.

Layer 2 Contains specific procedures to implement the basic security elements and activities of layer 3. The specification language ALMO$T [RHP99] was developed for that purpose.

Layer 1 Contains hard- and software building blocks specifically realizing any security requirement, basic security elements of case studies, and procedures of layer 2.

The evaluation process involves searching the repositories for any matching entries, beginning in the lowest, most specific layer: At first, the domain expert, who has only a limited knowledge of security-related concepts, models the business process and assigns high-level security requirements. Then, the expert checks whether there exists a soft/hardware building block (layer 1) or a procedure (layer 2), or at least a case study (layer 3) for each security requirement of each security object. If not, a dedicated security expert has to be consulted to either modify an existing or create a new case study representing the requirement. For each new or adopted case study, soft/hardware building blocks and/or basic procedures are developed and added to the repositories.

If that is not possible, the security expert informs the domain expert to either relax the requirements or remodel the business process. The process terminates when, for all security requirements, suitable low-level building blocks are either selected or newly created. The object-oriented security analysis tool SEMBA was developed to support this process.

$MoSS_{BP}$ was demonstrated mainly in the e-commerce domain: In [HH06] an electronic B2B transaction, the request for and the delivery of tenders, is analyzed for security requirements, whereas in [HP98] the application of the perspectives are illustrated on a typical order management process including digital signatures.

The main advantages of the $MoSS_{BP}$ framework lie in the process focus and the knowledge repositories. Focusing on business processes lays the emphasis on what are really important in business organizations, their business processes. The five perspectives allow for a simultaneous and detailed modeling of the processes and their security requirements, as well as adding security semantics to business models afterwards. Also, $MoSS_{BP}$ keeps the often costly consultation of dedicated security experts at a minimum, as domain experts usually have excellent knowledge of the business process and their security requirements, resp. their weaknesses. How to specifically model and implement the security measures can be determined by checking the repositories for suitable concepts, and security experts are only necessary if these concepts do not exist. But relying on the repositories too much may be disadvantageous; the concepts and patterns have to be kept up-to-date to include newly developed security measures, which would still require the consultation of security experts. $MoSS_{BP}$ also focuses solely on the technical implementation of safeguards and ignores other issues such as economical factors of safeguards (although SEMBA may consider safeguards costs as attributes) and specific threats and vulnerabilities (claimed to be as too tedious and laborious to deal with).

3.4. Security Attribute Evaluation Method - SAEM

The Security Attribute Evaluation Method (SAEM) proposed by Butler [But03], [But02] is a cost-benefit security analysis process based on a multiattribute risk assessment. As the risk assessment process is tasked with prioritizing threats, a benefit assessment determines the safeguard effectiveness, and a cost analysis determines the expenses associated with the security measures.

The SAEM process involves the following four steps:

1. Risk Assessment The risk assessment is structured such that multiple attributes are considered, relying on the Additive Value Model[5]: At first, all relevant threats are identified and so called Attack Outcome Attributes (e.g. lost revenue, lost productivity) are defined. These attributes are weighted according to their relative importance. Then, expected threat values are assigned to each threat for each attribute. These values can be both quantitative (e.g. lost revenue in monetary units) and qualitative (e.g. damage to public image using the Likert Scale). When all values are normalized to allow for direct comparison and the threats weighted with the attributes' weights, the resulting ranks are expressed in the Threat Index.

2. **Benefit Analysis** The next step is the benefit analysis where a prioritized list of security technology is created. After all safeguards are assigned to the threats they counter, their mitigation effectiveness is elicited. Then, for all safeguards, a new total threat index with modified threat frequencies and consequences (considering the mitigation effectivenesses) is calculated to take countering multiple threats by a single safeguard into account. The outcome is a ranking of security technology based on the importance and number of threats they counter.

3. **Coverage Analysis** After the benefit analysis, a coverage analysis is conducted to evaluate the overall mitigation of security threats. This coverage analysis is based on the defense-in-depth concept [SHF01] where multiple lines of defenses are suggested. Security managers should implement different types of security measures to reduce the vulnerability to threats. Butler defines the three defense lines of protection, detection, and recovery, and all identified safeguards are classified into one of these types. Thereby a graphic coverage analysis model that visualizes any uncovered areas can be developed for selected threats.

4. **Security Technology Tradeoff Analysis** Finally, the most suitable security measures can be determined with multiattribute techniques. As decision makers consider other properties of safeguards besides their threat mitigation effectiveness (determined in the benefit analysis phase), such as installation costs or maintenance efforts, for their final decision, the tradeoff analysis provides means to take those properties into account. Similarly to the benefit analysis, evaluation attributes are specified and ranked according to their importance, and the safeguards' ranks are calculated. The resulting list itemizes the safeguards subject to their cost-benefit efficiency.

[5] For more information on the Multiattribute Risk Assessment refer to [BF02].

Butler demonstrates the feasibility of SAEM in three case studies: The first case study is from a large commercial organization whose four IT departments are distributed throughout the world. The objective is to develop a global security architecture, as well as enforcing the consistency across the distributed IT departments. Compared to the overall size of the company, the security budget is relatively low. The second case study deals with a small local hospital that is connected to larger medical facilities via virtual private networks. No employee is dedicated to information security full-time and the hospital's security budget is very limited. Therefore, the main decision maker is tasked with finding the optimal security investments with respect to their budget, productivity, and the specifications of the Health Insurance Portability and Accountability Act (HIPAA). The third case study examines a large civilian governmental organization with several mainframe computers and a dedicated staff for security, including an incident response team. Although their security budget is very large, any security enhancing investments still have to be justifiable.

The SAEM approach is a very detailed and structured process to evaluate information security and safeguards. The risk assessment process ensures that specific threats are addressed, and the benefit and tradeoff analyses consider the multiobjectivity of threat consequences and safeguard effectiveness. The normalization of threat and safeguard values also allows the concurrent usage of qualitative and quantitative data. But, as the SAEM method is quite detailed and extensive, it is also rather complex to conduct. Each phase requires relatively much work and, without automation of certain steps, this work can be quite tedious. Furthermore, although the multiattribute risk assessment does allow for the definition of multiple objectives to be considered, the outcome is still aggregated into a single scalar value used for the evaluation, i.e. the threats and safeguards cannot be evaluated subject to the attributes 'independently'. Also, SAEM does not include any consideration of business processes and the safeguards' influence on them.

3.5. The CORAS Framework

The CORAS Framework is a tool-supported and model-based risk analysis methodology, the result of the EU-funded CORAS project [IST07]. The framework is founded on four pillars [SdBF$^+$02]: Risk Documentation Framework, Risk Management Process, Integrated Risk Management Process and System Development Process, and Platform for Tool Inclusion.

The main pillar of interest, the risk management process, is based on the AS/NZS 4360[6] and ISO/IEC 17799[7]. In contrast to specifying its own methods, the CORAS risk management process relies on techniques of other frameworks for each of the steps (see below) including HAZard and OPerability study (HazOp), Fault Tree Analysis (FTA), Failure Mode and Effect Criticality Analysis (FMECA), Markov analysis, and the CCTA Risk Analysis and Management Methodology (CRAMM). To provide a framework for modeling all risk-related aspects, a UML profile was developed [LHSS03] to act as a graphical reference and communication method between the different stakeholders.

The risk management process consists of the following steps [AdBD$^+$02], [FKG$^+$02]:

1. **Establish Context** At first, the context of the analysis has to be identified: The areas of concern are structured into scenarios that are usually of low detail level. This includes the SWOT (strengths, weaknesses, opportunities, threats) concern, the organizational context concern, and the target concern. Additionally, assets, as well as security requirements, are identified, evaluated, and summarized in the assets and requirements concern.

2. **Identify Risks** The next step consists of the specification of risks: Threats to assets are modeled in threat scenarios contained in the threat concern. Focus also lies on the unwanted incident concern, misbehavior caused by threats. Vulnerabilities to assets are considered in the vulnerabilities concern.

3. **Analyze Risks** After being identified, the risks are analyzed, i.e. their consequence and likelihood of occurrence evaluated. The consequence concern contains consequence estimates and descriptions of all unwanted incidents. The unwanted incident frequency concern contains a frequency model with frequency estimates of unwanted incidents, as well as descriptions of possible causes.

4. **Risk Evaluation** Next, the risks are evaluated with the following concerns: The risk estimates concern, risk priorities concern, risk theme concern (categorizing the risks in groups depending on the means to be prevented), and risk-theme relationship concern (interrelationships and dependencies between risks). Finally, the risk themes are ranked in the risk-theme priority concern.

5. **Risk Treatment** In the final step of the risk management process, risk treatment options are identified. Possible methods include security policy changes (security

[6] Australian/New Zealand Standard AS/NZS 4360:1999: Risk Management

[7] ISO/IEC 17799: 2000 Information technology - Code of practice for information security management

policy concern), strengthening the security requirements (security requirements concern), changes to the security architecture (security architecture concern), improving testing methods (testing concern), and describing requirements to monitor the system (monitoring concern). In conclusion, alternative prioritized solutions are searched in the treatment priority concern.

The CORAS approach was tested in several field trials during the development phase to provide feedback on the application of the individual risk assessment techniques and their interaction, and the CORAS framework itself. The trials were situated in the e-commerce (user authentication, secure payment mechanism, and autonomous agents for purchase) [DRRS02] and in the telemedicine domain (tele-consultation application ATTRACT, web-based collaboration service, eHealth service in HYGEIAnet) [SHL$^+$02], [SSH$^+$03], [SCS$^+$03].

The CORAS risk management process represents a holistic framework for the evaluation of information security of different application areas. It inherits all strengths and weaknesses of the assessment methods it incorporates, and the graphical models are the perfect tools for describing the target system, its context, and all security features, and therefore provide a valuable insight into the subject and facilitates communication between the stakeholders [AdBD$^+$02]. The combination of different analysis methods also reduces the individual weaknesses and therefore enhances the overall quality of the risk assessment outcome. But this integration also poses a considerable drawback of the CORAS approach: As it is recommended to rely on multiple methods in the same process step to get a more complete result, this also means an increased demand for time. Generally, the CORAS methodology is very time consuming, and the participants need experience in the multiple methods to be able to select and apply them efficiently.

3.6. CCTA Risk Analysis and Management Method - CRAMM

The CCTA[8] Risk Analysis and Management Method (CRAMM) [Ins07] is a commercial qualitative risk analysis methodology developed by the UK government's Central Computer and Telecommunications Agency in full compliance with the BS7799. It focuses on the technical aspect of security and is supported by a tool, now available in Version 5.1, distributed by Insight Consulting. CRAMM is divided into the three stages Asset

[8] Central Computer and Telecommunications Agency

Identification and Valuation, Threat and Vulnerability Assessment, and Countermeasure Selection and Recommendation. The CRAMM process includes the following steps [Bor04], [cra05] (fig. 3.2 [Ins07]):

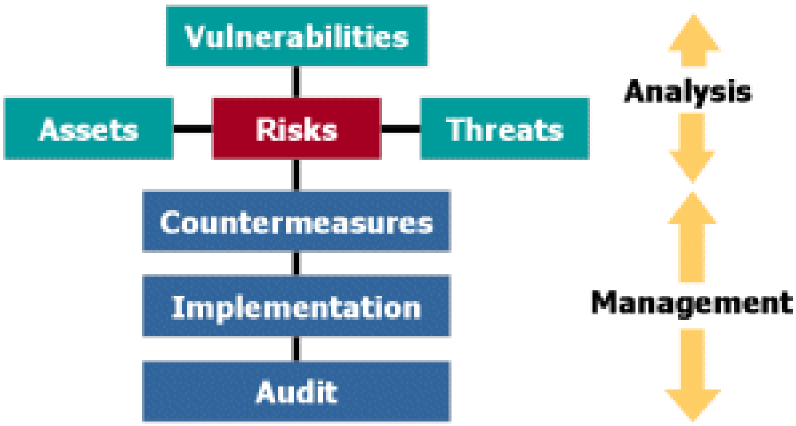


Figure 3.2.: CRAMM Process Steps

1. **Assets** Assets can be one of the following: physical, software, data, and location assets. Physical assets are valued on their replacement costs, intangible assets, such as data and software, are measured in terms of the business impact if they are compromised. Then assets are grouped into so called Asset Groups.

2. **Threats** Threats are determined by their relevant asset group (threats are not assigned to individual assets) and their level. The latter is determined by their possible frequency, measured in a qualitative 5-point scale from very low to very high.

3. **Vulnerabilities** Vulnerabilities are measured similarly to threats, but their levels only encompass 3 steps: low, medium, and high.

4. **Risks** After the asset identification and the threat and vulnerability assessments, the elements are combined into risks to calculate the measure of risks. These measures are defined in a risk matrix.

5. **Countermeasures** After the risk assessment, the CRAMM tool automatically recommends suitable countermeasures out of the library of 3500 controls. Controls are suitable, if they mitigate the correct threats, protect the correct assets, and if their security levels are appropriate for the risks (7-point from very low to very

high). The countermeasures are grouped into several logical groups which are divided into several 'security aspects'.

6. **Implementation** The next step is to implement the safeguards recommended in the previous step. Still, the risk analyst has to take several aspects into account that are not considered by CRAMM, e.g. safeguards mitigating multiple risks and the organizational environment.

7. **Audit** All steps can be reviewed if required.

The CRAMM methodology is especially suited for larger governmental organizations and commercial companies [eni06]: some of the clients include the London Borough of Newham, the Postal Services Commission (Postcomm), Smartwater Technology, and The Stationary Office (TSO) [Ins07].

The CRAMM framework is a well established methodology for risk assessment and is the British government's standard. But being valid for many commercial products, the CRAMM framework requires profound expertise to produce accurate results [Ins07], which means that often external qualified CRAMM practitioners are needed. This reduces the organization's internal staff's involvement in the assessment phase and therefore also does not improve their insight into security matters. The outcome is often quite extensive and a full review may last very long, up to several months. The framework neither offers the flexibility to customize it to the organizations characteristics, nor does it provide an evaluation of business process related issues. Grouping the assets into asset groups may also prove to be unfavorable, as all assets have their own properties and security requirements [Vid04]. And finally, CRAMM does not produce important economic numbers, such as implementation costs of the recommended safeguards and whether they fit into the security budget.

3.7. Operationally Critical Threat, Asset, and Vulnerability Evaluation - OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [CER07] is a risk-based strategic assessment and planning technique for security developed by the Carnegie Mellon University. Essentially, the OCTAVE framework is a set of criteria containing guidelines and requirements for implementing process steps, instead of pre-specified techniques. These criteria must be fulfilled in order to correctly implement the OCTAVE framework.

Unlike other frameworks, the OCTAVE approach is more focused on organizational risks instead of on technological ones and is structured into three phases [ADSW03]:

Phase 1: Build Asset-based Threat Profiles In this organizational evaluation phase, an exhaustive examination of the organization is conducted to identify all relevant assets. Their number is then reduced to the critical assets that are regarded as most important, and security requirements are specified for these assets. Finally, threats to the critical assets are identified and prioritized, and corresponding threat profiles are created.

Phase 2: Identify Infrastructure Vulnerabilities Whereas the first phase is aimed at an organizational evaluation, the second phase is geared to the technical aspects of the organization where the information infrastructure is being evaluated. IT components of the organization's network related to each critical asset are identified and aggregated into classes. They are then analyzed for any vulnerabilities and their extent. This evaluation can be automated by several software tools, e.g. network scanning.

Phase 3: Develop Security Strategy and Plans The third phase of the OCTAVE approach is the risk management process where risks to the assets are specified and analyzed for their impact on the organization. This analysis is the basis for the development of a protection strategy including risk mitigation plans and action lists.

As the OCTAVE framework is centered around the requirements criteria, specific methods have to be revised at first. To facilitate the practice of OCTAVE, three specific methodologies were developed, all compliant with the criteria [CER07]:

OCTAVE Method The first methodology developed is the so called OCTAVE Method, an implementation method suited for larger organizations (300 employees and more), taking advantage of knowledge from multiple levels of the organization. The method implements eight specific processes and takes the multi-layered hierarchy and the global distribution of large organizations into account, e.g. OCTAVE Method includes a formally structured and workshop-based data gathering step in phase 1. Current version is 2.0.

OCTAVE S For smaller organizations (about 100 employees and less), the so called OCTAVE S was developed that requires a team of only 3-5 participants to conduct the whole assessment process. To better suit the needs of smaller organizations, OCTAVE S's phase 1 is more streamlined, and phase 2 is also abbreviated because small organizations are often outsourcing computer maintenance. The current version of OCTAVE S is 1.0 (preliminary version).

OCTAVE Allegro Recently, a third method was developed, the so called OCTAVE Allegro method (a variant of OCTAVE Method), which is aimed at organizations focused on information assets (about 100 employees and less). It exclusively deals with information assets and how they are used and processed, and the threats and vulnerabilities they are exposed to. Like the other methods, OCTAVE Allegro can be conducted in a workshop-style, but can also be done by individuals without extensive organizational involvement. 1.0 is the latest version.

The OCTAVE framework was applied in several different research areas such as health care [Col04], where the organizations of interest were a small US Hospital in Europe, a medium sized specialty care hospital group and research center in the Eastern US, and a distributed group of 45 community/regional facilities in the Mid-Western US. Another application was demonstrated by Nevo and Kim [NK06] where the OCTAVE framework was applied to perform risk analysis for Internet voting and other forms of voting.

The OCTAVE approach is a risk assessment framework that allows a high level of adaptability for the organizations, either in choosing one of the pre-specified methods or in designing an individual set of processes for their own needs. Unlike e.g. CRAMM, it is self-directed (as defined in the OCTAVE criteria), i.e. the organizations' internal staff conducts all the necessary steps and therefore gains valuable experience and insight. Relying on workshops and drawing on the expertise of employees of different domains, the results are thorough and detailed. But OCTAVE is not suited for getting those results fast, especially with the OCTAVE Method: It is claimed that it can be conducted within 2-3 weeks, but it can also last up to several months, as the workshops are very time consuming. The OCTAVE S methodology may be completed in 2-3 days, given adequate preparatory material, but appointing a workshop for the 3-5 participants (having sufficient knowledge of their organization), may be a difficult task, especially for small distributed organizations. OCTAVE Method does not consider the likelihood of threats (due to the fact that this data is often not available); S allows a qualitative assessment of threat likelihoods. Finally, OCTAVE does not specifically address business processes and, as a strategic evaluation method focused on organizational instead of on technical aspects, does not provide any decision support for selecting specific security measures.

3.8. Facilitated Risk Analysis and Assessment Process - FRAAP

The Facilitated Risk Analysis and Assessment Process (FRAAP) was developed by Peltier [Pel05] to streamline and simplify the risk assessment process. It is structured as a qualitative risk analysis framework that is driven by business managers and relies on in-house experts as FRAAP team members. Emphasis lies on the facilitator who guides the participants through all the process steps. Prior to the FRAAP, a Pre-screening phase takes place to define a set of baseline controls and the business objectives of the enterprise. This phase serves as an evaluation, whether a full scale risk assessment or just implementing baseline controls is necessary, based on the sensitivity of the information objects and the impact of their disclosure/destruction on the business activities. Supposing that a risk assessment is required, the FRAAP is conducted:

Pre-FRAAP Meeting The pre-FRAAP meeting's purpose is to define the scope and target of the assessment (including the identification of the assets) and the discussion of organizational issues. This includes appointing the FRAAP team members and time schedules, reviewing the pre-screening results, creating a visual diagram displaying the information flow of the process (visual reference), and agreeing on crucial definitions (such as CIA, threats, and controls). Pre-defined checklists ensure the completeness of the Pre-FRAAP deliverables.

FRAAP Session The actual FRAAP session is divided into two stages: Stage one covers identifying threats, establishing risk levels, and documenting possible controls; stage two deals with identifying all existing controls and assigning new ones. Stage one begins with an introduction that may follow an agenda where all important issues are addressed. After these preliminaries, threats are identified and risk levels assigned, based on their likelihood of occurrence and impact (expressed in terms of levels, e.g. high, medium, and low). The risk levels are then determined by a risk matrix, ranging from A to D (A: must be treated, B: should be treated, C: requires monitoring, D: negligible). For all A- and B-level threats, suitable mitigating controls are then identified using different sources such as ISO 17799 or the Sarbanes-Oxley Act (SOX). After all possible safeguards are determined, stage two commences, where existing controls are identified for all threats of level A and B. For any threat currently not being treated, new controls are assigned and responsibilities defined.

Post-FRAAP In the final FRAAP-phase, a final report for the management is generated containing the outcome of the FRAAP session. The documents include a management summary report containing key findings of the assessment, a detailed action plan that specifies implementation schedules of the new controls and otherwise accepted risks, and a cross-reference report where the controls are listed together with their threat relationships. This report is used as the basis for the final decision on which new controls are to be actually implemented.

The FRAAP was practiced at several organizations including the GLBA Bank where the security of Nonpublic Personal Customer Information held and/or processed at GLBA was assessed [Pel05].

The FRAAP framework is a flexible and adaptable risk assessment methodology that relies on in-house stakeholders as FRAAP team members. Its main assets are its independence from external security experts and analysts (apart from the facilitator) and its flexibility (can be easily adapted to the particular needs of different organizations). Its requirements in time consumption are also quite moderate, as the whole process can be completed within several days, in contrast to other methodologies (e.g. CRAMM). A possible drawback may be the focus on the facilitator: The success of FRAAP is highly dependent on the quality and expertise of the facilitator who guides the FRAAP participants through all process steps. This team leader has to have profound business and information security knowledge, as well as important soft skills such as being able to listen, support, guide, and settle disputes. And finally, FRAAP is not supported by a software tool, and the assessment focuses on the technical capabilities of controls only and therefore does not allow the evaluation of safeguards according to other aspects (costs, user acceptance).

3.9. Comparison and Summary

The Analytic Hierarchy Process (AHP) is a widespread and easy to use decision support tool for evaluating different alternatives that can be applied to solve security safeguard selection problems. Its strength is the analysis of the alternatives' properties in different categories, or in other words, the evaluation of alternatives with respect to multiple objectives. That means that different characteristics of alternatives, security safeguards in the context of information security, like their ability to ensure confidentiality or their maintenance costs, are recognized and accounted for, respecting the multiobjective nature of the safeguard selection problem. The pairwise comparison technique however requires the direct comparability of alternatives, which may pose a problem. As security safeguards are not limited to technical solutions but also include organizational measures and operational procedures, comparing them directly may be problematic, e.g. comparing a packet filtering firewall with a fire extinguisher. Therefore, it may be beneficial not to use the AHP as a standalone tool for solving information security-related problems, but to integrate it with other methods (e.g. [SH03]).

Another framework that takes multiple objectives into consideration when determining suitable security safeguards is the cost/benefit-based Security Attribute Evaluation Method (SAEM). Unlike AHP, it has been developed specifically for solving information security evaluation problems and therefore particularly addresses security-related concepts such as threats and safeguard effectiveness. Multiobjectivity is accounted for in the multiattribute risk assessment where threats are ranked according to their likelihood of occurrence and impact on attack outcome attributes. The resulting threat index values and the effectiveness values of the security technologies under consideration are then used to calculate their risk reduction impact. The coverage analysis ensures that no security gap is overlooked when arranging the safeguard portfolio, and the tradeoff analysis compares the risk reduction impact and other benefits of security measures with their costs like implementation or maintenance costs.

The qualitative risk analysis and assessment methodologies CCTA Risk Analysis and Management Method (CRAMM), Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), and the Facilitated Risk Analysis and Assessment Process (FRAAP) also include specific threats in their evaluation process and define risks in a traditional way as the combination of assets, vulnerabilities, and threats, in contrast to SAEM which completely ignores assets in its multiattribute risk assessment. The asset-driven risk assessment frameworks ensure that the focus lies on the elements in need for protection.

The commercial risk analysis framework CRAMM is intended for large governmental and commercial organizations. It provides a structural method to identify relevant assets (arranged into asset groups), possible vulnerabilities, and threats, to combine them to risks that are measured according to the assets' values and vulnerability and threat levels, and to recommend suitable countermeasures. The process is considered as rather complex and considerable experience is required in order to produce meaningful and correct results. Therefore, organizations often rely on external qualified CRAMM practitioners to conduct the analysis instead of letting internal analysts undergo the extensive training to gain the necessary expertise.

OCTAVE is quite different to CRAMM: On the one hand, the actual OCTAVE framework does not provide a step by step procedure as CRAMM, but a set of criteria that has to be met to conform to the OCTAVE methodology. This provides great adaptability and more flexibility than CRAMM to address specific organizational needs. For easier access, three specific application methods have been developed to choose from, suited for different sizes of organizations. On the other hand, it is self-directed, meaning that the OCTAVE methodology has to be wholly exercisable by the organization's internal staff in a workshop environment, thus not relying on external experts. Finally, OCTAVE is focused on organizational risks, whereas CRAMM concentrates more on technical issues, and OCTAVE generally does not take threat likelihood into consideration (except for OCTAVE S which provides basic means for including threat likelihood in the evaluation).

What both approaches have in common is that they both require a great deal of time; a full analysis and review can last up to several months (except for OCTAVE S aimed at small sized companies). The Facilitated Risk Analysis and Assessment Process (FRAAP) is better suited for getting fast results. It has been developed to streamline and speed up the risk assessment process and to reduce the complexity of other risk-based frameworks. Like OCTAVE, FRAAP is structured as a workshop with company internal experts as participants, but also requires a (mostly external) facilitator to guide the discussions. Asset values are not analyzed separately, but influence the impact of threats. Economical attributes of security controls such as acquisition costs are completely neglected in the evaluation process (same as CRAMM and OCTAVE).

While the risk assessment methodologies evaluate security technologies on their effectiveness to mitigate risks, the Process-Oriented Security Models (POSeM) and Modeling Security Semantics of Business Processes ($MoSS_{BP}$) frameworks deal with information security in a different way. They take into consideration that assets do not generate business value themselves, but participate in business processes that produce utility, and therefore the methodologies rely on business processes as the basis for their analysis. They also ignore specific harmful events (i.e. threats), but concentrate on eliciting security requirements and deriving appropriate security measures. Although both are aimed at improving business process security, their individual approach taken is completely different.

POSeM is a rule-based method to analyze the requirements of process components (actors, activities, artifacts) for confidentiality, integrity, availability, and accountability, measured in qualitative scales. The first rule base ensures that security levels are sufficiently high for actors and activities to handle artifacts, and the second allows the derivation of suitable security safeguards according to the required security levels of process components. The rule bases are adaptable to specify any safeguard dependencies or other company specific constraints (e.g. separation of duty principle). In contrast to risk-based approaches, POSeM ignores any specific malicious incidents and only considers intangible assets such as data (as artifacts).

As already stated, $MoSS_{BP}$ also focuses on process models but makes use of UML models to define hardware/software building blocks or conceptual mechanisms to conform to security requirements of business processes. These concepts are stored in repositories of different abstraction levels. $MoSS_{BP}$ has been developed with the aim to reduce the participation of expensive external security experts to a minimum. The domain expert, usually having only limited knowledge of information security-related issues, defines high level security requirements and relies on the repositories to find concepts how to realize the solutions. The security expert only needs to be consulted if such concepts are not present. As with POSeM, threats and vulnerabilities are completely neglected in the $MoSS_{BP}$ framework.

The final methodology in this list is the CORAS framework that also applies UML for modeling security-related issues, but is centered around a traditional risk assessment process with asset, vulnerability, threat identification and evaluation and safeguard derivation. In order to model the risk entities, a UML profile has been developed. Unlike the other methods, CORAS incorporates techniques of other frameworks to realize its risk identification process including HAZard and OPerability study (HazOp) and Fault Tree Analysis (FTA). This ensures a thorough analysis of the problem, but also requires participants proficient with these techniques to pick the most appropriate.

This comparison reveals that all methodologies focus on certain aspects of information security only and neglect others, thus not being able to provide a complete security evaluation of a business process and multiobjective safeguard selection. The risk-based approaches take assets and threats into account and therefore consider specific risks in the analysis, but neglect business processes. POSeM and $MoSS_{BP}$ in turn are process-based, but ignore specific threats and risks. None of these frameworks consider multiple criteria when evaluating the safeguards, except for AHP and SAEM. But AHP is not specifically developed to deal with security-related issues, thus lacking information security specific functionality. And SAEM can be considered as a hybrid, including methods for multiobjective optimization and risk determination, but not as thorough as the other risk-based methods, and also lacks business process support.

4. Design of a Model-Supported, Risk-Based Multiobjective Decision Making Process

In this chapter, the main contribution of this thesis is presented, a methodology for a risk assessment based on process models and security safeguard selection. Whereas other existing frameworks often concentrate on a certain aspect of security and do not address all requirements for the definition of Secure Business Processes, this approach provides a holistic methodology for eliciting security-related elements based on business processes, measuring the risks, and choosing an optimal safeguard portfolio to ensure business process security. It is a model-supported, risk-based multiobjective decision making process (MR-MOD) and incorporates elements of different disciplines and their strengths:

Model-based Elicitation Process Process models are used for deriving security relevant assets and threats they are exposed to.

Risk Assessment A risk assessment process provides a structured method to measure information security risks and to valuate security safeguard effectiveness.

Workshop A workshop environment ensures consideration of the different opinions and expertise of different participating domain experts such as security experts, process owners, and other stakeholders.

Multiobjective Decision Making A multiobjective decision making process takes multiple criteria into consideration and provides solutions that represent the best tradeoffs of opposed factors.

The MR-MOD framework consists of three distinctive phases, each of them divided into several sub-steps (figure 4.1):

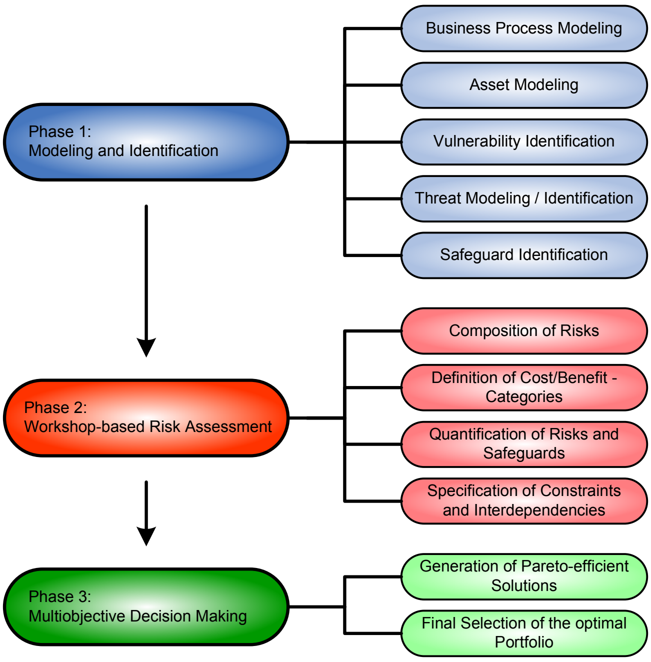

Phase 1:
Modeling and Identification
Business Process Modeling
Asset Modeling
Vulnerability Identification
Threat Modeling / Identification
Safeguard Identification
Phase 2:
Workshop-based Risk Assessment
Composition of Risks
Definition of Cost/Benefit - Categories
Quantification of Risks and Safeguards
Specification of Constraints and Interdependencies
Phase 3:
Multiobjective Decision Making
Generation of Pareto-efficient Solutions
Final Selection of the optimal Portfolio

Figure 4.1.: Overview of the MR-MOD Phases

Phase 1: Modeling and Identification The first phase is tasked with the modeling and the identification of all security relevant entities, based on business process models.

Phase 2: Workshop-based Risk Assessment In the next phase, risks are composed, cost and benefit categories are defined, and related values assigned to all relevant entities, as well as constraints and interdependencies specified.

Phase 3: Multiobjective Decision Making The final phase deals with the generation of Pareto-efficient solutions, their analysis, and the final selection of the optimal safeguard portfolio with respect to the cost/benefit categories.

This approach picks up the concept of combining a risk assessment process with multiobjective decision making in a workshop environment and further develops the Multiobjective Security Safeguard Selection Tool (MOS^3T) Workshop Process proposed by Neubauer et al. [NSW06] to define Secure Business Processes [NKB06] by adapting and extending this concept to be able to deal with process security. The underlying idea and purpose of this proposed framework is to determine the effectiveness of security safeguards to reduce risks to assets, but also to include the influence of safeguard implementation on the business processes in the analysis. Together with other properties of the security measures like user acceptance or acquisition costs, these effects are to be considered when deciding on the optimal security portfolio for the given business process.

This framework is intended to support the decision makers of organizations in gathering and evaluating the information needed to determine suitable security investments. It provides a step by step process to collect and analyze the required data with a risk assessment process which includes the consideration of assets worth to be protected and specific threats they are exposed to (risk assessment methods are applied with great success [Pel05]). Finally, it proposes some efficient candidate portfolios for the decision makers to choose from, based on the outcome of the risk assessment process.

As the focus lies on the protection of business processes, process models are used to identify assets crucial for the process activities and threats to the process. While using these models as the starting point for the analysis, decision makers can ensure that they do not overlook the core processes of their business activities that are vital for generating value. This also accounts for the process-centered view of today's business. After all relevant components are identified, they are analyzed in a quantitative manner. This requires the collection of numerical data, which is often hard to come by. Hence, this framework relies on the expertise and experience of different participants from different areas of the organization, e.g. security and IT experts, process owners, members of the management, and other decision makers. To support their collaboration, the risk assessment is structured as a workshop process. When all entities have been rated and all participants agree on the assessment, candidate portfolios are generated by testing all possible portfolio combinations of safeguards for Pareto-efficiency considering their different properties, measured in different categories. This multiobjective optimization ensures that all relevant aspects of safeguards are taken into consideration when deciding on the optimal solution.

As already stated, this framework incorporates the risk reduction effectiveness of safeguards, as well as their influence on the business processes in the analysis. Risks are defined as threats exploiting certain vulnerabilities to attack assets and can be mitigated by certain security technologies. Assets are determined by their value, vulnerability by their exposure, threats by their likelihood of occurrence, and safeguards by their effectiveness. Asset value, vulnerability exposure, and threat likelihood determine the risk value (cf. figure 4.2).

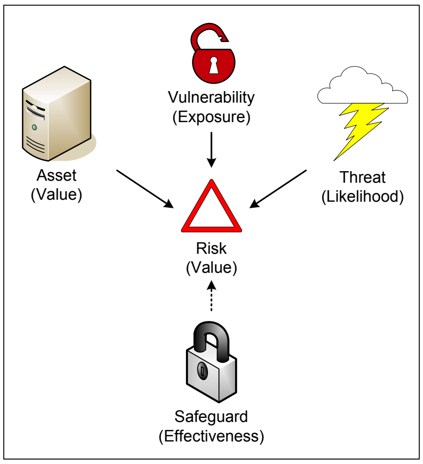


Figure 4.2.: Relation of Assets, Vulnerabilities, Threats, and Safeguards

The other main property of safeguards apart from their risk reduction effectiveness is their influence on business processes. This influence can be explained as follows: While safeguards protect assets that are required for business processes to work and thereby preserve asset value, they indirectly affect process activities and their outputs as well. The loss or breakdown of an asset may result in reduced productivity or even a complete stop of business activities. By ensuring the assets' availability for the process (and preventing unintended tampering), safeguards contribute to the utility value business processes generate. But safeguards not only have a positive effect on processes, but also can have a negative impact on them by reducing the productivity e.g. due to increased cycle times. Figure 4.3 sketches the safeguards' influence on business processes.

As a proof of concept, a software tool is developed to assist the decision makers in the MR-MOD process.

In the next sections, each phase of MR-MOD is presented in the following way: At first, a short summary is given including characteristics and goals of the particular phase and required participating roles. Then each sub-step is explained in detail and an example is given for illustration purposes.

4.1. Modeling and Identification

The first phase, Modeling and Identification, serves as a preparatory phase prior to the workshop-based risk assessment. It is tasked with the modeling of business processes and the modeling and identification of the entities needed for the risk assessment: assets,

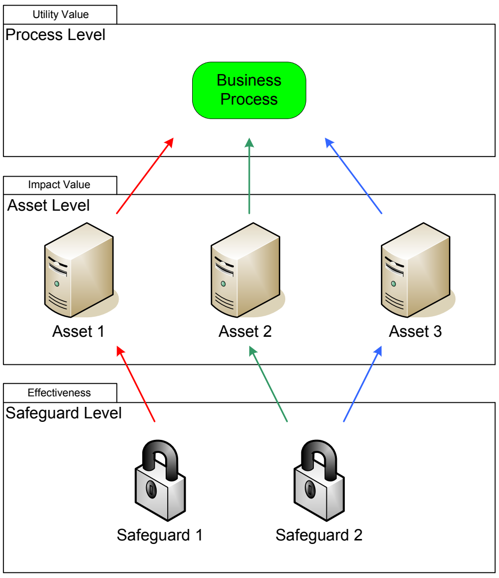


Figure 4.3.: Safeguard Impact on Processes

threats, vulnerabilities, and possible safeguards. Participating roles should be (chief) process owners having specific domain knowledge of the processes and IT/security experts. If required, a modeler may be consulted additionally.

This phase is done prior to the workshop process in order to save time. As it is often difficult to bring certain stakeholders together, the sub-steps of this phase can be conducted iteratively: The CPO and the modeler devise the process model, identify the assets and figure out some threats; then the security expert defines vulnerabilities and further threats; the CPO adds further assets and the security expert adds corresponding vulnerabilities and so on. That way the roles do not need to be physically present at the same time.

Within the scope of the MR-MOD framework, modeling is done with the aid of the Adonis toolkit and a modified version of the Standard Application Library (Student Version 2.0 - 3.53, cf. Appendix A.1.3).

4.1.1. Business Process Modeling

Since the business process is the basis of this security evaluation, a model (diagram) of the business process (or part of a business process) is required. Of course there is no need to specially develop a model for the MR-MOD framework if a suitable diagram is already at hand, e.g. as the result of a minor process improvement or a full scale business process reengineering (BPR) effort. In that case, this model can be used. Otherwise, security-related issues can be integrated with the remodeling process where certain aspects should be considered, such as choosing an either top-down or bottom-up approach and following modeling guidelines [Pid03].

At first, the participants have to agree on the level of detail which has to be followed throughout the whole modeling process, because this affects how assets are perceived in the next step of MR-MOD. The granularity of the model defines whether certain activities are broken down into sub-activities or aggregated.

Example The following simple order processing workflow of a company selling goods over the Internet serves as an example: The process starts with receiving the order for a particular product. The first task for the processor is to check the stock on hand for availability of the product. If not, the order handling process stops. Otherwise, a shipping order is send to the delivery department and then the process stops. The process owner is tasked with developing a process model of low detail for the analysis. The outcome is a diagram with two activities (figure 4.4).

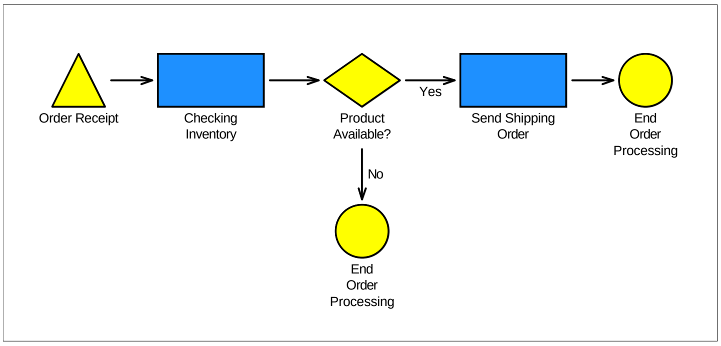


Figure 4.4.: Exemplary Order Handling Process

4.1.2. Asset Modeling

The next step consists of identifying and modeling all process-relevant assets. Therefore, the process model developed in the previous step is extended with all assets that are related to the particular process. This includes tangible as well as intangible assets, e.g. servers and confidential customer data. Besides the process's size and complexity, the number of identified assets also depends on the detail level of the process model: If

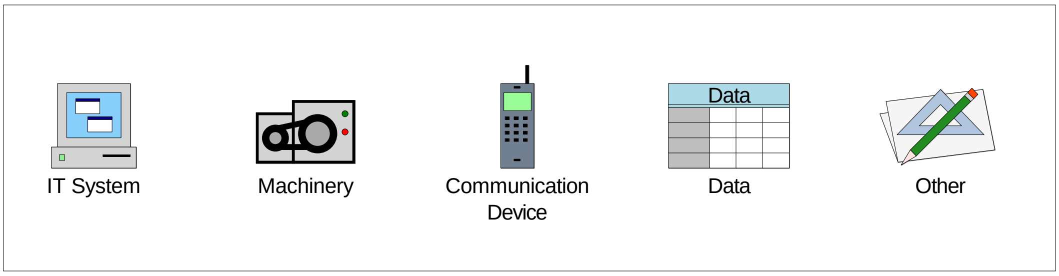


Figure 4.5.: Asset Types

the detail level is high, major assets may be split up into several assets, e.g. customer-related data into personal data, order history, and account information, which would be modeled as the single asset 'customer data' otherwise.

For this step, the Standard Application Library shipped with the Adonis toolkit has been extended with the so called Asset-extended Business Process Model, a modification of the standard Business Process Model diagram type. This modification includes the definition of different asset types:

IT System This type refers to all sorts of IT hard- and software, ranging from application and database servers to printers, monitors, and application software.

Machinery Machinery corresponds to machines other than IT systems, such as production machinery.

Communication Device Communication Devices include all means of communication and collaboration between persons.

Data Intangible assets such as customer data, production plans, or technical manuals are modeled as data type assets.

Other For all other assets that do not fit in any of the previous classifications, the type Other is defined; e.g. the expertise of a domain expert falls into this category.

This categorization is used to improve the clarity and structure of the process/asset model and therefore helps to identify all crucial assets. Technically, this differentiation has no further effects on the risk assessment process; all assets are dealt with in the same way. Figure 4.5 shows the graphical representation of the categories.

When all important assets are identified, they can be assigned to specific activities of the business process. Like the categorization, this mapping only serves to improve the model's readability and provides no additional input data for the risk assessment.

Example Analyzing the order handling process, the domain expert identifies the following assets worth being protected: the processor's workstation (IT system), the customer's order request (data), and the inventory database (data). Figure 4.6 shows the process model extended with the assets mapped to the activities. For a higher detail level, further assets may be customer data, application server and software, database server, and network infrastructure.

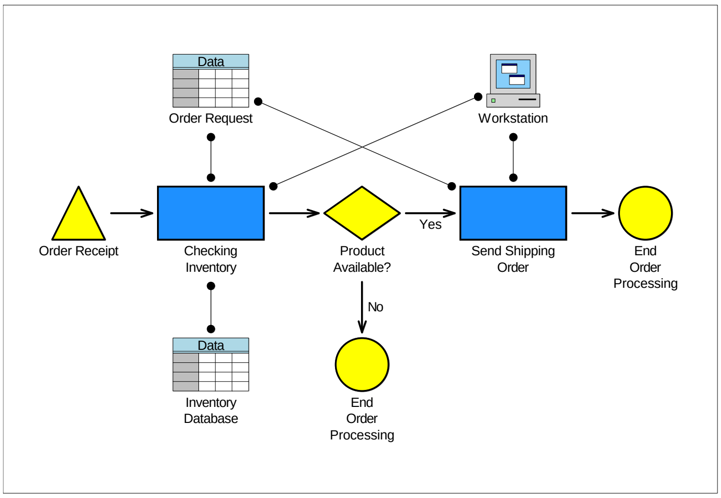


Figure 4.6.: Order Handling Process extended with Assets

4.1.3. Vulnerability Identification

After identifying and modeling all assets, they are analyzed for any vulnerability they are exposed to. Of course a single vulnerability may be relevant for different assets, as well as an asset having several vulnerabilities. Therefore, no direct assignments of vulnerabilities to assets are realized yet (this is done later in the workshop) to avoid redundant entities.

Established existing vulnerability listings (e.g. found on the Internet or developed by other organizations) may be conferred to in order to check for completeness of the own vulnerability list. Examining the security properties (CIA) of the assets, i.e. which of the CIA properties are relevant for the assets and checking for corresponding vulnerabilities, can be another aid in that process.

Example The security expert examines the assets identified by the process owner and recognizes some considerable vulnerabilities: Although a basic malware scanner has been installed on the workstations, signatures are not updated on a regular basis, thus reducing the scanner's effectivity. Furthermore, the processor generally lacks security awareness, leaving the workstation in the logged on status. And backups of the database are not done according to a fixed schedule, leaving it prone to data loss.

4.1.4. Threat Modeling / Identification

After the identification of all applicable vulnerabilities, all specific threats that may exploit the vulnerabilities to cause damage are identified. Again, existing threat listings may be utilized to complete the threat list. For modeling purposes, the concepts of Misuse and Abuse Case models [MF99], [SO00], derivations of the well known Use Case models, are adapted. This adaption includes the replacement of the actors with threat agents (human, system, or other) and the specification of harmful and undesired events, both intended and unintended, as Abuse and Misuse Cases. The differences between the two model types are:

- Misuse Case models (figure 4.7) represent all threats that are resulting from a misuse of the system by legitimate and authorized persons, i.e. not intended faults such as mistyped characters or accidental deletion of important data. Additionally, natural threats and adverse incidents that are not caused by humans like fire or hardware failure are also modeled as Misuse Cases.

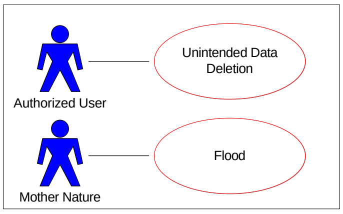


Figure 4.7.: Misuse Cases

- Abuse Case models (figure 4.8) represent all threats that are generated by possible attacks of human threat agents, i.e. intended abuse of the system such as hacker attacks, viruses, worms, and others. Threats not directly related to human threat agents such as botnets or malicious servers are also modeled here as they are run or developed by humans with malicious intensions.

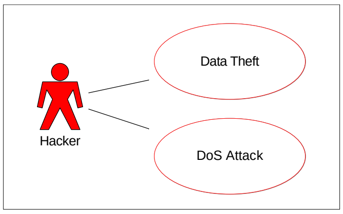


Figure 4.8.: Abuse Cases

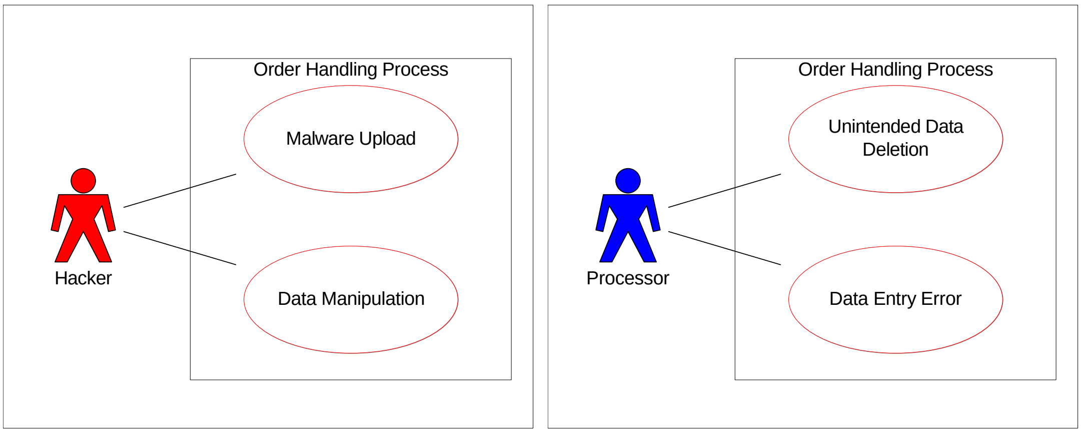


Figure 4.9.: Miuse and Abuse Cases of the Order Handling Process

Misuse and Abuse Case Diagrams are modifications of the Use Case Diagram type of the Adonis Standard Application Library (cf. Appendix A.1.3). Technically they are identical, except for the color of the actor: Threat agents in the Abuse Case diagrams are colored red, whereas the actors of the Misuse Case diagrams are blue to distinguish their different intentions. The purpose of explicitly modeling Misuse and Abuse Cases is to illustrate the harmful incidents and who causes them. Especially for non-security experts, the easy-to-read use case model diagrams are suitable for improving their awareness of security critical events.

Example The security expert identifies hacker attacks and associated data leakage or destruction as the main threats. Another probable adverse event may be a data loss due to hardware failure. The process owner however is concerned about data entry errors by the processor or unintended data manipulation, e.g. deletion of data sets. Those thoughts are collected and modeled as misuses and abuses with two different threat agents, the external hackers and the internal processor (figure 4.9).

4.1.5. Safeguard Identification

The final step of the first phase is the Safeguard Identification process where all available safeguards are identified. These safeguards are the candidates for the final security portfolio and the main elements to be evaluated in the MR-MOD framework. The other elements identified and collected in the preceding sub-steps are used to determine the safeguards' effectiveness in risk mitigation. That and the other categories the safeguards are valued in are specified in the following risk assessment phase.

Basically, security safeguards are not solely technical solutions (e.g. encryption) but also include non-technical measures that reduce the impact or probability of risks. Similarly to vulnerabilities and threats, the resulting list may be checked against available safeguard checklists in order to generate a complete enumeration of available security measures (e.g. ISO 27001). Security experts may define a classification of safeguard types (e.g. as found in [Pel05]) for clarity reasons.

Example In this final step of the identification phase, the security expert and the process owner work together to collect a list of suitable safeguards. For purposes of clarity, the security expert decides to separate the security measures into technical and operational/organizational safeguards. The technical measures include malware scanners of different vendors, different firewall types, and encryption techniques. Operational/organizational measures are the introduction of employee training sessions to increase the processor's security awareness, periodic backups, and virus signature updates on a regular basis.

4.2. Workshop-based Risk Assessment

In the second phase, the information gathered in the first phase is used as input material. The main tasks are the composition of risks as asset/vulnerability/threat-tuples, the definition of cost/benefit categories based on security/dependability and monetary objectives, and the assignment of values to risks and safeguards as needed for the defined categories. Additionally, assets, threats, vulnerabilities, and safeguards are checked for completeness, any possible missing element is added, and constraints and interdependencies of safeguards are defined. The information collected in this phase serves as the input for the next phase, the multiobjective decision making process.

A major difficulty here is the lack of quantitative data about risks and/or safeguards such as the rate of occurrence of risks. Therefore, the main source of information is the experience/expertise of the participating members of this assessment process. That means that participants need to be from many different areas of the company, contributing their knowledge to get the most accurate data. The risk assessment process is realized as a workshop environment that proved to be quite successful in dealing with multiple opinions and preferences of different stakeholders [Gru00]. Multiple points of view also ensure completeness of the input data. Other available data sources may be logs, surveys, universally valid standards, and such.

To be effective, many different roles need to be participating in this phase: external or internal IT/security experts, (chief) process owners, members of the upper and lower management division, accountants, system users, and other important stakeholders.

4.2.1. Composition of Risks

At the beginning of phase 2, the asset, threat, vulnerability, and safeguard lists are reviewed because workshop participants also include additional stakeholders other than the process owner and IT/security expert of the preceding phase. These additional participants usually bring in other components such as assets that are not obvious at first glance, but are nevertheless crucial for the process, e.g. the business process participants' expertise may be regarded as an important asset to be protected against the threat of social engineering. Apart from other threats and vulnerabilities, especially non-technical safeguards that are not necessarily security-related, are likely to be identified at this stage. An example would be the improvement of the working environment enhancing employees' working atmosphere, thus lowering the probability of employees to commit deliberate internal attacks against the company due to dissatisfaction. Not being a security-related 'technology' at first sight, this measure is capable of reducing the risk of internal attacks and increasing the security of the company, therefore qualifying as a security safeguard.

When all participants agree on the completeness of the elements' lists, the actual risk composition step commences and risks are defined by assigning individual vulnerabilities and threats to assets, resulting in a collection of asset/vulnerability/threat-tuples. These tuples are then assigned safeguards that are capable of countering the specific risks. A single safeguard may be mapped to multiple risks, as well as a single risk countered by multiple safeguards. Equally, the assets, vulnerabilities, and threats may be part of multiple specific risks.

Basically, the risk composition can be accomplished in two different ways:

- Generating all possible asset/vulnerability/threat combinations, dropping all impossible tuples (e.g. asset 'employee expertise' with vulnerability 'no backups' and threat 'fire') and only keeping the valid ones. This ensures that all possible combinations are considered, but it may also result in a considerable work load, depending on the number of risk components.

- Breaking down the assets/vulnerabilities/threats lists into functional groups (e.g. threats to hardware-based assets or threats to software-based assets) and therefore only applying risk combinations technically possible. This requires greater diligence because of components belonging to multiple groups and therefore increasing the chance of overlooking a valid tuple, but this method also presents a more structured approach of eliciting all possible risks.

Assigning safeguards to risks is better done with the latter method, because safeguards tend to be risk specific, only mitigating a limited number of risks. This first step of the second MR-MOD phase terminates when all participants agree on the completeness and correctness of all risk tuples and assigned safeguards.

Unlike other risk management frameworks, the MR-MOD approach basically separates the identification of risk components and their assessment to reduce the duration of the workshop phase, as it is often difficult to schedule appointments which all required participants are able to attend. Concerning the identification of relevant risk components, this step has only review purposes and therefore should not take too long.

Example For the risk assessment phase, additional stakeholders apart from the process owner and security expert, including business process participants and members of the management division, join the team and begin composing the components to specific risks. The IT and security expert concentrates on technical risks (e.g. malware-related attacks) and the others on procedural risks (table 4.1).

Table 4.1.: Some Risks of the Order Handling Example

Risk Name	Asset	Vulnerability	Threat
Malware Infection	Workstation	No Virus Sign. Updates	Malware Upload
Sabotage by Internal Threat Agent	Inventory Database	Employee Dissatisfaction	Deliberate Data Destruction
Data Entry Error	Order Request	Carelessness	Error Overlooking

The safeguards assigned to the exemplary risks are listed in table 4.2.

Table 4.2.: Safeguards assigned to Order Handling Risks

Malware Infection	**Sabotage (Internal Threat Agent)**	**Data Entry Error**
Regular Scanner Updates	Working Environment Improvements	Employee Training Sessions
Malware Scanner A	Logging	
Malware Scanner B	Regular Backups	

4.2.2. Definition of Cost/Benefit Categories

The next sub-step involves the definition of the cost and benefit categories the safeguards are to be rated in and which reflect the properties of safeguards that are of interest for decision makers. Whether their capability of asset value preservation, maintaining confidentiality of assets, or the amount of time needed for their maintenance are criteria for deciding for or against a particular security measure, this can be defined as either a cost category, if the corresponding value should be minimized (e.g. maintenance costs), or a benefit category, if the corresponding value should be maximized (e.g. effectiveness of safeguards to maintain CIA attributes). The diligent specification of these categories is of vital importance as these categories should generally reflect the corporate strategy and security policy of the company: A large commercial bank has a high demand of security measures that assure confidentiality, whereas a small non-profit organization would certainly concentrate on other factors such as keeping the costs of security investments at a low level. Considering the variety of different organizations, there exists a multitude of different possible categories that are company specific and individually customizable, ranging from monetary quantities (e.g. minimizing the reduction of monetary loss, monetary costs) to intangible values (e.g. user acceptance, loss of reputation).

While the categories are basically company specific, they actually conform to certain characteristics of safeguards, i.e. their capability to mitigate risks threatening assets, their either positive or negative influence on the business process, and other non-risk- or non-process-related attributes. To address these aspects, three distinctive category types are defined, while safeguard values for each of these types are calculated differently relying on their own set of input data:

Risk-Related Category Risk-related categories directly refer to risk reducing values of safeguards and rely on quantitative data on assets, vulnerabilities, threats, and safeguard effectiveness to calculate the category values. Input data includes asset value, vulnerability exposure, threat likelihood of occurrence as ARO, and safeguard effectiveness[1] for each risk-related category (figure 4.10).

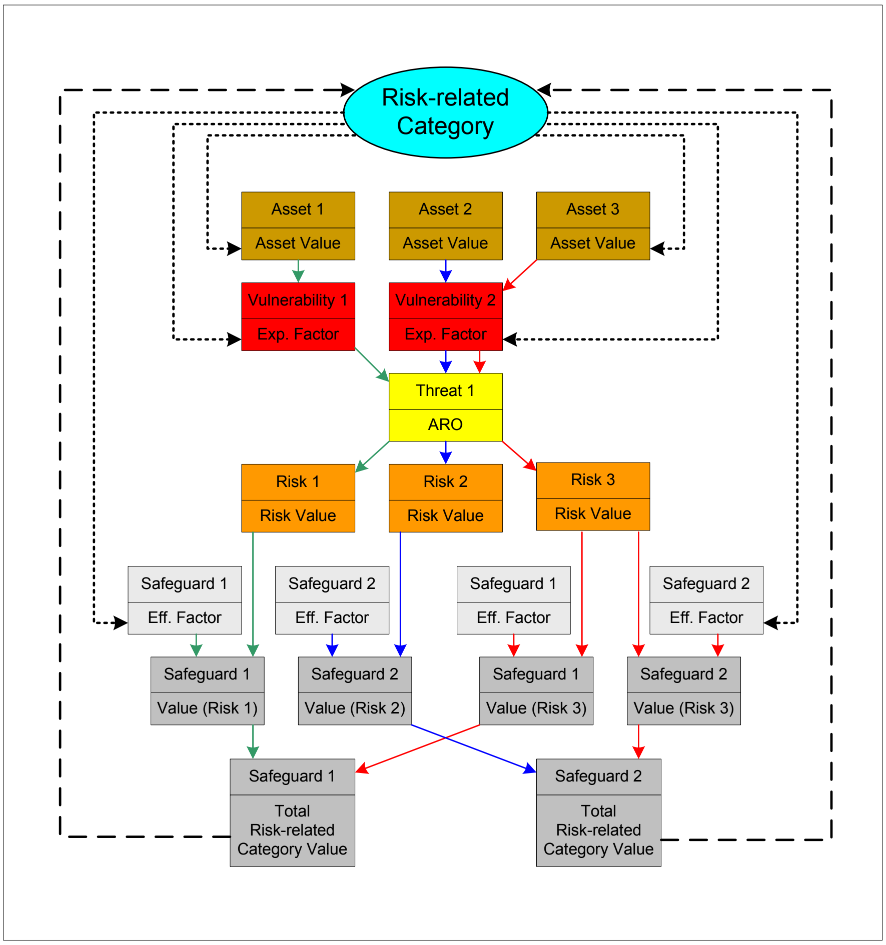


Figure 4.10.: Risk-related Category Type

This type is suited for expressing monetary values as well as immaterial ratings (e.g. CIA properties). Risk-related safeguard values are determined by the following formula:

$$RC_{j,k} = \sum_{i=1}^{n}(AV_{i,j} \times \frac{EXP_{i,j}}{100} \times ARO_i \times \frac{EFF_{i,j,k}}{100}) \tag{4.1}$$

where $RC_{j,k}$ is the risk reduction capability of safeguard k in category j, $AV_{i,j}$ the value of the asset assigned to risk i in category j, $EXP_{i,j}$ the exposure factor of the vulnerability of risk i in category j (in percent), ARO_i the annual rate of

[1] Safeguard effectiveness is also determined individually for each assigned risk.

occurrence of the threat of risk i ($ARO_i \geq 0$), $EFF_{i,j,k}$ the effectiveness factor of safeguard k to reduce the value of the risk i in the category j (in percent), and n the total number of risks safeguard k counters. Note that this formula resembles the ALE-function, but the RC-value is not restricted to monetary values.

Process-Related Category Process-related categories refer to the impact of safeguards on the utility value generated by a business process, depending on the asset impact, which is the relative importance of an asset for the execution of a process, and the process-related safeguard effectiveness, the capability of the safeguard to ensure the asset's availability for the process (figure 4.11).

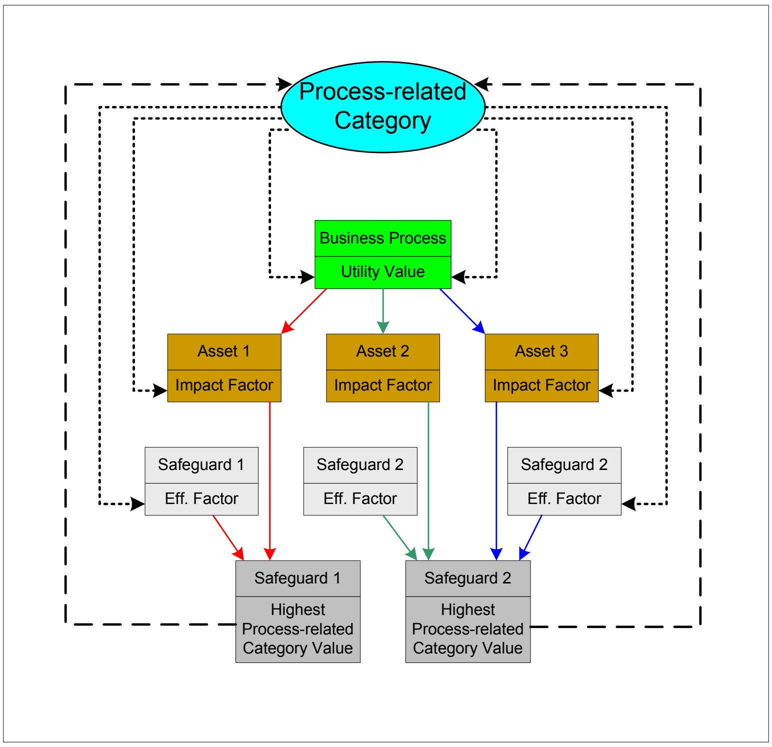


Figure 4.11.: Process-related Category Type

Typically, this utility value is measured in monetary terms, but is not restricted to it. Process-related safeguard values are calculated as follows:

$$PC_{j,k} = \max(U_j \times \frac{IMP_{i,j}}{100} \times \frac{PEFF_{i,j,k}}{100}) \quad for\ i = 1...n \tag{4.2}$$

where $PC_{j,k}$ is the process contribution value of safeguard k in category j, U_j the utility value generated by the process in j terms, $IMP_{i,j}$ the impact factor of asset i on the utility value j (if the asset does not contribute to the utility value at all, the impact factor is set to 0, contrariwise a value of 100 indicates that the loss or breakdown of a particular asset would lead to a complete halt of the process), $PEFF_{i,j,k}$ the process-related effectiveness factor of safeguard k to protect asset i in category j (in percent), and n the total number of assets safeguard k protects. If a single safeguard protects multiple assets and therefore generates multiple PC values, max denotes that the greater value is used for the evaluation[2].

Simple The remaining fall into the simple category type where safeguard values are represented by single scalar values, $SC_{j,k}$ for safeguard k in category j, and no calculations for determining the values are needed (figure 4.12). This includes all sorts of categories that are not directly related to risks or processes, e.g. user acceptance or acquisition costs, and they can be measured in any preferable unit.

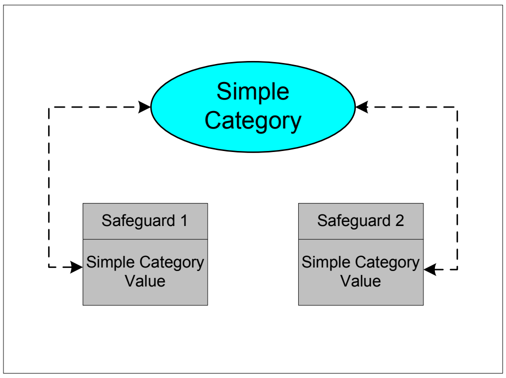


Figure 4.12.: Simple Category Type

To sum it up, the category types are applied as follows: While risk-type categories measure the value of the assets themselves (and therefore the risk-reducing capabilities of safeguards to preserve asset value), process-type categories measure the impact of safeguards on the value generated by a business process (through asset impact and asset/safeguard mappings). Simple-type categories are related neither to risks nor to processes and solely refer to safeguards.

Actually, assets, vulnerabilities, and threats are only needed to be identified when risk-related categories are defined (assets are also necessary for process-related categories).

[2] These denominations are only suitable for benefit categories; for cost categories the denominations have to be modified, while the actual formula remains valid (cf. section 6.3 - cost category definitions).

For simple categories, only safeguards are to be identified. But, as risk components are the core elements of this framework, it is highly recommended to define at least one risk-related category to include these elements in the evaluation process.

Example The decision makers are interested in how well the safeguards fare in protecting the assets, what benefit they provide for the order handling process, and how much they cost. Therefore, they decide on defining the following categories as decision criteria:

- Risk reduction capability of safeguards (risk-type benefit) measured in monetary terms.
- Process benefit of safeguards (process-type benefit) measured in points.
- Implementation costs (simple-type cost) measured in monetary terms.

4.2.3. Quantification of Risks and Safeguards

After defining the cost/benefit categories, the risks and safeguards are assigned appropriate quantitative values. The specific values required depend on the defined categories e.g. the safeguards' acquisition costs if minimizing these is an objective, or the relative influence of a certain risk on a corporate's asset confidentiality level. The required quantitative data for each category type is as follows:

Risk-related Category Asset Value, Vulnerability Exposure (in percent), Threat ARO, risk-related Safeguard Effectiveness (in percent)

Process-related Category Process-generated Utility Value, Asset Impact (in percent), process-related Safeguard Effectiveness (in percent)

Simple Category Safeguard Value

This sub-step is the most difficult task of the whole workshop process. Generally, accurate quantitative data is lacking or incomplete, therefore this methodology relies heavily on the expertise of different stakeholders and their experience to accurately estimate necessary data. That is the main reason to structure the risk assessment phase as a workshop process, namely to include the knowledge of different experts and to aggregate their experience into a precise picture of the organization's security situation. The process is intended as an informal open discussion to avoid any unnecessary overhead, but can be structured in any way (e.g. EasyWinWin [Gru00]) should the need arise.

For the discussion, it is beneficial not to appoint a certain moderator for the whole risk assessment phase, but to let the participant with the most extensive knowledge of the elements currently discussed guide the particular steps, e.g. asset value -> process owner, threat ARO and vulnerability exposure -> security expert, safeguard costs -> accounting manager, etc.

Other possible sources of information are any available logs, surveys, standards, or other either publicly available or company-owned documents that can be used in the workshop.

Example By consulting the statistics of the expenditures of the last periods and tenders made by security product vendors, the accounting manager comes up with acquisition cost estimates for all technical safeguards. The costs of the operational security measures are determined by the other stakeholders. Threat- and vulnerability-related data, as well as safeguard effectiveness values, are elicited by the security expert relying on security logs and industrial standards, and the process owner estimates the process generated utility value. The other numbers are determined by general discussion. E.g. the outcome for the risk 'Malware Infection' is composed as follows: Workstation Value (1500 monetary units), No Virus Signature Updates (40% exposure), Malware Upload (ARO of 10), resulting in a risk value of 1500 x 0.4 x 10 = 6000 monetary units. When considering the safeguard 'Regular Scanner Updates' with an effectiveness rating of 90%, the resulting safeguard value in the risk reduction capability category is 6000 x 0.9 = 5400 monetary units per year with an acquisition cost of 0 monetary units for the scanner already in use.

4.2.4. Specification of Constraints and Interdependencies

The final but somewhat important sub-step of the second phase is the specification of constraints and interdependencies. These rules can be used to model constraints and effects such as restrictions in the number of security technology of the same type to be included in the valid portfolios or reduction of implementation costs for getting safeguards of the same vendor. Three types of constraints and two types of interdependencies are defined:

Category Constraint Category constraints refer to restrictions of safeguard portfolio values, i.e. the aggregated values of safeguards included in the portfolios for each category that must not be violated. For benefit categories, minimum border values are specified, maximum border values for cost categories.

Inclusion Constraint Inclusion constraints refer to the minimum number of safeguards out of a given set that have to be included in the solution. That way, any must-haves or already implemented safeguards that should be kept may be specified.

Exclusion Constraint Exclusion constraints work the other way round, referring to the maximum number of safeguards to be included. A possible usage of this constraint is to make sure that only one out of multiple firewalls (of different vendors) is included in the solution.

Minimum Interdependency Interdependencies refer to a defined number of safeguards out of a given set that is needed to trigger certain synergy or cannibalism effects that alter the solution value in a specified category. The minimum type defines the minimum number of safeguards. For example, acquiring multiple safeguards (virus scanner and firewall) from the same vendor would result in a reduction of acquisition costs (discount).

Maximum Interdependency The complement to the minimum type, a portfolio has to include at most the specified number to trigger the effect on the category value.

Example The management dictates that the implementation costs must not exceed 10000 monetary units. Therefore, the category constraint for the cost category 'implementation costs' is set to 10000 units, implying that aggregated safeguard costs of a portfolio must not exceed a value of 10000 units in order to be valid. Additionally, it is determined that at least one malware scanner has to be part of the portfolio, which is realized as an inclusion constraint with the required candidate count of 1 out of the following safeguard list: malware scanner A, malware scanner B. To indicate that only 1 firewall should be present in order to prevent problems, an exclusion constraint is defined with a candidate count of 1 out of the set of available firewall products. Finally, vendor B would grant a discount, if the stakeholders would decide on acquiring both malware scanner and firewall suites from this vendor, modeled as a minimum interdependency with a candidate count of 2, the safeguard list consisting of malware scanner B and firewall B, and the reduction of the portfolio costs by the granted discount.

4.3. Multiobjective Decision Making

The third and final phase of the proposed methodology is the multiobjective decision making process using the predefined cost/benefit categories as objectives and the quantitative data gathered in the preceding phase as input. The output is a list of all non-dominated solutions, i.e. safeguard combinations not violating any restrictions.

The roles needed for this phase are chief decision makers and any required advisors.

4.3.1. Generation of Pareto-efficient Solutions

The search for the optimal solutions relies on the concept of Pareto-optimization and works as follows:

Enumeration All possible combinations of safeguards are enumerated and the solution values for each objective are calculated. This includes pre-calculating risk- and process-related values with their corresponding input data and determining the portfolio values for each category which is done using one of the following aggregation types:

- Total (sum) of all individual safeguard values:

$$PV_{j,p} = \sum_{k=1}^{n_p} (SV_{j,k}) \tag{4.3}$$

  where $PV_{j,p}$ is the value of portfolio p in category j, $SV_{j,k}$ the individual values of safeguard k in category j ($RC_{j,k}$[3] for risk-related, $PC_{j,k}$[4] for process-related, and $SC_{j,k}$ for simple categories), and n_p the total number of the safeguards included in portfolio p.

- Average of all individual safeguard values:

$$PV_{j,p} = \frac{\sum_{k=1}^{n_p} (SV_{j,k})}{n_p} \tag{4.4}$$

- Minimum of all individual safeguard values:

$$PV_{j,p} = \min(SV_{j,k}) \quad for\ k = 1...n_p \tag{4.5}$$

[3] cf. formula 4.1

[4] cf. formula 4.2

- Maximum of all individual safeguard values:

$$PV_{j,p} = \max(SV_{j,k}) \quad for\ k = 1...n_p \tag{4.6}$$

Validation Any synergy and cannibalism effects of solutions are applied and solutions that violate any restrictions, such as exceeding a maximum cost level or violating any inclusion/exclusion constraints, are discarded.

Pareto-Dominance The remaining portfolios are analyzed for dominance: Each new solution is compared to the temporary solution set (current set of non-dominated solutions) by a pairwise comparison, and if it is better in at least one objective and equally good in all others, it is declared as dominating and included in the solution set, while the other now dominated solution is dropped. If the new solution is dominated i.e. worse in at least one objective, but not better in any other, it is dropped. Otherwise, it is declared as non-dominated and added to the list. The resulting list defines the global optima of the solution space.

The effort in enumerating all possible solutions depends on the number of candidate safeguards, with a total number of 2^n combinations. While the enumeration can be done by hand for a very small number of candidate safeguards (e.g. 4), a higher candidate count requires computer-aided calculation, i.e. the MODStool prototype software introduced in the next chapter.

Example For illustrating the concept of Pareto-dominance in determining the efficient solutions, the following three portfolios are examined (table 4.3)[5]:

Table 4.3.: Exemplary Candidate Solutions

Portfolio	Risk Reduction Value	Process Benefit	Implementation Costs
Portfolio A	5000	3000	6000
Portfolio B	15000	8000	9000
Portfolio C	10000	4000	6000

Having implementation costs below the category constraint of 10000 and assuming that no safeguard constraints are violated and all interdependencies considered, all three portfolios qualify for being tested for Pareto-dominance. Beginning with

[5] Higher values are better for the risk reduction and process benefit categories, lower for the implementation costs; values are aggregated with the total-type.

portfolio A, which is compared with B, B has considerably better values in the categories risk reduction and process benefit, but is worse in category implementation costs. Therefore, both portfolios are considered as non-dominated. Comparing A to C, C is better in risk reduction and process benefit and equally good as A in costs, thus being better in at least one category and not worse in all others. Therefore, A is now dominated by and replaced with C. B is neither dominating nor being dominated by C, hence remaining non-dominated.

4.3.2. Final Selection of the Optimal Portfolio

After acquiring all non-dominated solutions, the final decision has to be made, based on the preferences and experience of the decision makers. All solutions are further analyzed and the list of portfolios shortened by imposing stricter category constraints until the optimal portfolio remains, the one that suits the needs of the decision makers best.

Example The decision makers analyze both portfolios B and C (table 4.3) and discuss which is better. While B provides better results in maintaining asset value and a higher process benefit, C is less costly. Naturally, members of the management prefer the latter solution, but the security expert stresses the importance of keeping the assets secure. Therefore, being sensitized to information security-related problems by the workshop process, the other stakeholders agree and decide on implementing the safeguards of portfolio B.

The whole MR-MOD process can be conducted on a regular basis to reevaluate the current situation of business process security. If required, only certain steps can be done as well (e.g. if new safeguards are developed and the safeguard portfolio needs to be reevaluated without reanalyzing risks). When done properly, this process presents an easy way of selecting the most appropriate safeguards to certain needs and provides a clearer understanding of the processes used. The modeling part helps in getting a better view of the business processes and supports decision makers that are no IT/security experts to understand security-related issues better, thus sensitizing them to security matters.

5. Development of a Software Tool supporting the Proposed Methodology

As a supplement to the proposed MR-MOD methodology, a MultiObjective Decision Support tool (MODStool) was implemented to aid the risk assessment and decision support process. It was developed as a Microsoft Windows application that connects to a relational database hosted on a Microsoft SQL Server (2005) for permanently storing data. Apart from the security safeguard evaluation, this tool also supports other types of multiobjective decision support sessions, such as the evaluation of non-security specific IT investments for business processes. The MODStool makes use of the INNOV library and the ATANA Visualization Tool [NS07a], [NS07b], [NSW06]. The INNOV tool is responsible for finding the non-dominated portfolios by enumerating all possible combinations and dropping the dominated and constraint-violating ones. It uses ASCII-textfiles for data input and output. The ATANA application is a graphical representation tool for the non-dominated solutions and allows the analysis of the portfolios by modifying upper and lower bounds.

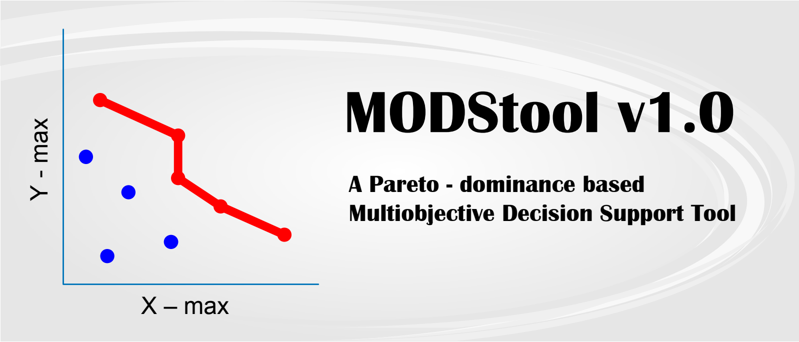

MODStool v1.0
A Pareto - dominance based
Multiobjective Decision Support Tool
Y - max
X – max

Figure 5.1.: Splash Screen

In the following sections, the structure and functionality of this tool is presented in detail.

5.1. Requirements

5.1.1. Main Requirements and Features

The main purpose of the tool is to support the MR-MOD workshop and multiobjective decision support phases and to provide functions implementing all sub-steps of these phases. That includes the definition of the following elements and their attributes:

Benefit / Cost Categories Name, type (risk, process, simple), unit, dimension (multiplier), aggregation type (for analysis), generated utility value, constraint

Assets Name and comment (asset type), asset value for each risk-related category, impact factor for each process-related category

Vulnerabilities Name and comment, exposure factor for each risk-related category

Threats Name, ARO, and comment (threat type)

Risks Name, specified asset, vulnerability, and threat, assigned safeguards

Safeguards Name and comment, safeguard effectiveness for each risk and risk-related category, safeguard effectiveness for each asset and process-related category, safeguard values for each simple category

Inclusion / Exclusion Constraints Name, candidate count, assigned safeguards

Minimum / Maximum Interdependencies Name, candidate count, category and effects, assigned safeguards

Solutions Safeguards included in the solution, aggregated safeguard values for each category

Additionally, the following requirements have to be met:

Sessions All data collected for a certain risk assessment and decision situation has to be saved in sessions. This allows the storage and handling of different scenarios with their specific data. Additionally, different decision support session types, along with the security-related risk assessment, should be possible (i.e. IT investment evaluation).

Permanent storage of data Data accumulated during a decision support session has to be stored permanently for later reevaluation. To accomplish this, the tool is connected to a Microsoft SQL Server 2005 and stores necessary information in a relational database.

Import of XML data from Adonis Apart from manual input, the tool also has to support the import of assets and threats from XML files generated by the Adonis tool in the Modeling and Identification phase of the MR-MOD methodology.

Import/Export of XML data generated by MODStool Additionally, it has to provide functions to export and import elements to/from XML files generated by MODStool.

Evaluation and Optimization After collecting all necessary data, the tool has to evaluate the safeguard candidates according to the specified categories and optimize the safeguard portfolios by finding all non-dominated combinations.

Graphical Representation and Analysis Finally, all solutions have to be graphically presented for further analysis. This includes the comparison of the newly found optimal portfolios with each other, as well as with the set of safeguards currently in use.

5.1.2. Workflow

The following steps present the typical usage of the tool in the course of a risk assessment and decision session. Screenshots of the GUI and further explanation of the individual functions and elements can be found in the functionality section (section 5.2).

1. Creation of a new or Opening an existing session

After starting the tool, the first step is to create a new session or to open an existing one (either original or copy).

2. Definition of the Model Properties

In the next step, the properties of the decision session are defined, including the definition of benefit and cost (or resource) categories, candidate safeguards, assets, threats, vulnerabilities, and risk mappings.

Benefit and cost categories are specified by their ID, description, and unit (with multiplier). It is also set here whether the categories are to be optimized and which analysis method (aggregation type) to use. Categories are divided into the required three types: risk-related, process-related, and simple.

Risk-related categories are the main part of this tool that rely on quantitative asset, vulnerability, and threat values, as well as safeguard efficiency values for evaluation. Actually, risk-related categories do not have to be specified, but are highly recommended for the evaluation of safeguard performance.

Process-related categories represent the impact of safeguards not on assets, but on business processes. They rely on the assets' participation in processes for evaluation. These categories are only usable if at least one risk-related category has been defined before because safeguards may not be directly mapped to processes, but indirectly through the risks they counter. Therefore, process-related benefit categories rely on the risk/safeguard mappings defined for the risk-related types.

Simple categories cover all the other criteria that may not be directly related to risks or processes. They do not require pre-calculations, but they directly refer to a simple scalar value specified for each safeguard.

For all categories, one of the following four aggregation types is selected: total, average, minimum, and maximum. Total simply sums up the values of the safeguards included in the solution for each category, average calculates the average value (determined by the value sum and the number of included candidates), minimum only considers the lowest value of all included safeguards of the category, and maximum is the opposite of minimum.

Assets, vulnerabilities, threats, and candidate safeguards are specified by their ID, description, and an optional comment. For threats, their ARO is specified as well. The quantitative data for the other entities is entered later in the data input step (see below). Safeguards currently present and deployed in the organization can be marked as so to compare the newly generated solutions to the current safeguard portfolio in use.

Apart from manual input, assets and threats can also be added by importing them from XML-files generated by the Adonis toolkit. Having selected the input file, the assets/threats are directly added to the database if they are not already present. Additionally, all elements can be exported to and imported from XML-files generated by MODStool, including any quantitative data. Additionally, all elements and their corresponding valuations can be directly imported from other sessions as well.

After defining assets, vulnerabilities, and threats, the risk tuples are generated by mapping a single vulnerability and threat to an asset. Then, all candidate safeguards that counter a specific risk are assigned to this risk. A safeguard may counter multiple risks and therefore may be assigned multiple times. These risks and safeguard mappings are only required by the risk-related and process-related categories.

3. Process Definition and Mappings

If process-related categories are defined, process information needs to be entered: For each category, a corresponding value that represents the value generated by the process has to be specified, as well as the impact factor of each asset. The impact factor measures the relative importance of an asset for the execution of a process. Then safeguard effectiveness values are entered. The product of process generated value, asset impact factor, and safeguard effectiveness yields the safeguards' benefit for the process (cf. formula 4.2). If the same safeguards are mapped to multiple assets, thus having multiple category values, the higher values are considered in the optimization process.

By defining multiple process-related categories, it is possible to analyze multiple processes. Asset mapping is realized through the impact factor: A value of 0 expresses no relation between an asset and a process; a value of 100 denotes that this asset is vital for the execution of the process and a loss or breakdown of the particular asset would lead to a complete halt of the process.

4. Data Input

The Data Input step includes entering all required quantitative data for all risk-related entities and safeguards (cf. section 4.2.3), depending on the pre-specified cost and benefit categories.

For all risk-related benefit categories, corresponding asset values, vulnerability exposure factors, and safeguard effectiveness factors are assigned. Note that the safeguard effectiveness is set for each risk individually; a safeguard may be more successful in countering a certain risk than another one. Analyzing the risks and their vulnerability exposure factors and threat AROs, the user may define which risks to include in the optimization process and which to ignore (some risks may be of lower importance, especially low impact/low rate of occurrence risks). Finally, all values for the remaining benefit and cost categories of the simple type are assigned to the safeguards. All these quantitative values are utilized for the non-domination evaluation, should their corresponding category be marked to be optimized. Otherwise, aggregated category values are only checked for any category constraint violations.

5. Definition of Constraints and Interdependencies

The next step consists of defining all interdependencies. Include and exclude constraints specify the minimum and maximum number of candidate safeguards out of a defined list that are to be included, AND and OR relations specify the minimum and maximum number of safeguards out of a list to trigger the synergy and cannibalism effects. Constraints are indicated by their ID, description and the min/max number of safeguards, along with the safeguard list. For relations, the corresponding categories and the possible category value changes are defined additionally.

Furthermore, any category value restrictions that must not be violated are specified, including the minimum border for benefit values and the maximum border for resource categories. Note that the value restrictions are related to the analysis type, e.g. setting the minimum border of a benefit category marked as a minimum type means that all individual safeguards of a candidate portfolio must not violate this border in order to form a valid combination; for the total analysis type, the sum of all included safeguards values are measured against the border.

6. Calculation

The penultimate step consists of the determination of all non-dominated solutions that conform to all specified constraints and restrictions. This is conducted in two sub-steps: At first, the risk reduction capabilities of safeguards are calculated for all risk-related categories by multiplying the risk values, which in turn are determined by the product of value/exposure/ARO, with their corresponding safeguard effectiveness factors (if a single safeguard counters multiple risks, their values are summed up). For all process-related categories, the corresponding safeguard values are calculated by multiplying the utility value with the asset impact factor (of the assets the safeguards are mapped to) and the process-related safeguard effectiveness factor. All these values are saved in the database. Then, the actual search for optimal solutions by the INNOV library commences. It iterates through all possible combinations and checks them for any constraint violations. Average/total type analysis values are calculated including any synergy and cannibalism effects of relations, min/max values not. Valid solutions are tested for non-domination and only non-dominated portfolios are kept and finally saved to the database. For comparison, the category values of the currently deployed safeguard portfolio are calculated as well.

7. Analysis

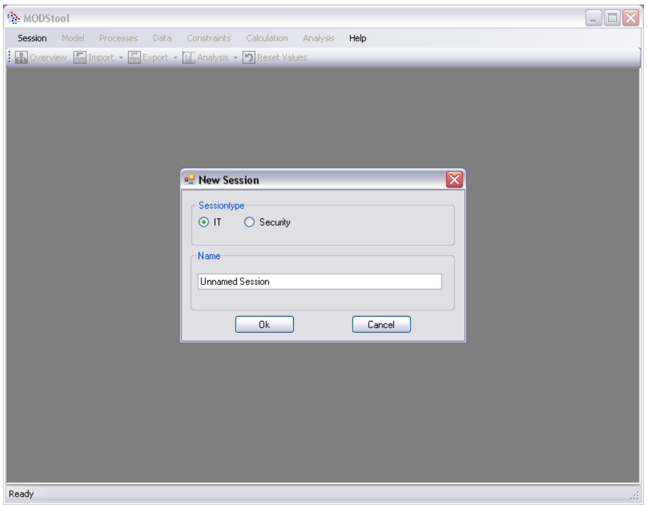
In the final step, all determined solutions are analyzed. The ATANA framework provides means to display all non-dominated solutions and allows the decision makers to alter the upper and lower borders at their discretion. By doing so, a final optimal portfolio can be determined according to the users' preferences.

5.2. Functionality

The major functions of this tool are aggregated to eight main groups: Session, Model, Processes, Data, Constraints, Calculation, Analysis, and Help. These functional groups are accessed via the top level menustrip items. On startup of the tool, only the main form with the top level menustrip is shown and only the Session and Help menuitems are available. After opening an existing or creating a new session, the other functions and their menustrip items become accessible. When clicking on the items, a corresponding sub-form is shown that provides the data manipulation functions. The sub-forms are further divided into multiple tabpages. While working on a specific sub-form, all the others are hidden from the user.

Alongside the major functions, some helper functions are accessed via a toolstrip: Overview shows a functional overview diagram for navigational purposes; Import contains items for importing all entities, both from XML files and other sessions; Export writes entities to XML files; Analysis allows access to functions and forms belonging to the ATANA visualization; Reset Values reloads the data of the current grid from the database to undo any temporary data modifications made by the user.

Commonly, the sub-forms (and their tabpages) contain two different types of elements: grids and buttons. Grids display the data and provide a table-like view of the entries with rows and columns for easy data manipulation. Some entries are directly editable in the grid itself (adding, deleting, editing), some are manipulated via buttons. ID entries are never editable, because IDs are used as unique identifier and are assigned by the database automatically. Generally, the data changes made by the user are saved to the database when the current tabpage is left, but some pages save on other occasions as well (cf. individual tabpage descriptions below). The name of the currently loaded session is displayed in the main form's header.



Sessiontype
● IT ○ Security

Name
Unnamed Session

Figure 5.2.: New Dialog

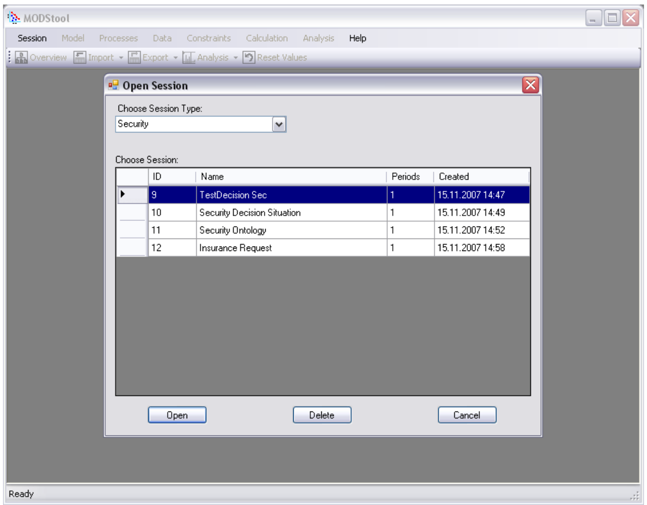
In the following, the individual functional groups and their tabpages are explained in detail.

5.2.1. Session

The Session menustrip item, the only other enabled on startup alongside Help, contains the following sub-items: New, Open, Open Copy, Rename Session, Close, Preferences, and Exit. New opens a dialog to create a new session from scratch. Open lets the user load and manipulate an existing session. Open Copy opens a copy of the selected session. Rename Session allows renaming the currently loaded session. Close stops the work on the current session and closes all sub-forms. In Preferences, several options for the analysis can be set, including New View, Present Value Markings, Period Number, and Rounded Axis Values. Exit stops the whole application.

The New Dialog lets the user choose the Security session type (and other types implemented in the tool) and the session description.

The Open/Open Copy dialog shows all sessions stored in the database, separated by session type. The user marks a session and clicks on the Open button to load the selected session (or the copy). No renaming of sessions is allowed here, but sessions can be deleted via the Delete button.



Choose Session Type: Security

Choose Session:

	ID	Name	Periods	Created
▸	9	TestDecision Sec	1	15.11.2007 14:47
	10	Security Decision Situation	1	15.11.2007 14:49
	11	Security Ontology	1	15.11.2007 14:52
	12	Insurance Request	1	15.11.2007 14:58

Figure 5.3.: Open Form

5.2.2. Model

The Model sub-form group allows the specification of the session specific entities: benefit and resource categories, candidate safeguards, assets, vulnerabilities, threats, and risks.

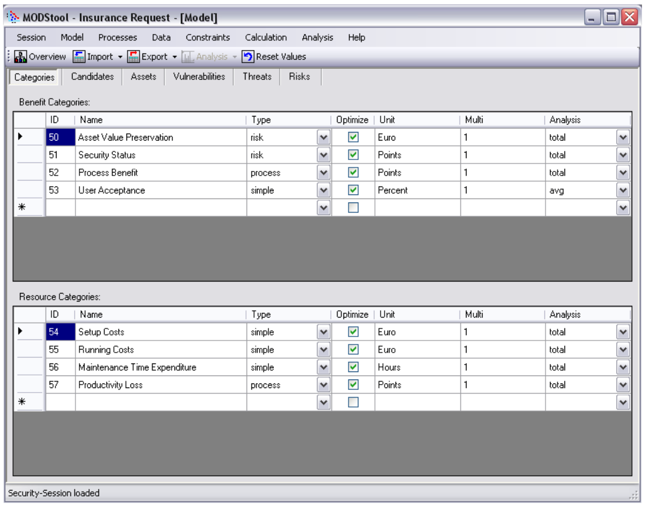
Category

The Category tabpage allows the definition of session specific benefit and resource categories.

The two grids show the benefit and resource categories. The user can create and delete rows directly in the grids and all columns except for the IDs are editable. The Type column specifies the type of category (risk-related, process-related, simple). Unit shows the units the categories are measured in. The Optimize column defines whether the category is to be optimized in the decision process or the candidate safeguards just checked for boundaries (specified in the Constraints sub-form). Multi refers to the dimension of the category values e.g. 1000 meaning that the specified value is 'in thousands'. The Analysis column defines the aggregation type out of total, average, minimum, and maximum.

Candidates

The Candidates tabpage shows the candidate safeguards including their ID, the mandatory name, and an optional comment. The user may add, delete, or alter an entry directly in the grid. Currently Present specifies whether the specific candidate is part



Benefit Categories:

ID	Name	Type	Optimize	Unit	Multi	Analysis
50	Asset Value Preservation	risk	☑	Euro	1	total
51	Security Status	risk	☑	Points	1	total
52	Process Benefit	process	☑	Points	1	total
53	User Acceptance	simple	☑	Percent	1	avg
			□			

Resource Categories:

ID	Name	Type	Optimize	Unit	Multi	Analysis
54	Setup Costs	simple	☑	Euro	1	total
55	Running Costs	simple	☑	Euro	1	total
56	Maintenance Time Expenditure	simple	☑	Hours	1	total
57	Productivity Loss	process	☑	Points	1	total
			□			

Security-Session loaded

Figure 5.4.: Model - Categories

of the currently deployed portfolio. The currently deployed portfolio represents the candidates that are already in place and describes the portfolio the other newly found solutions are compared to (in addition to each other). Thereby, the decision maker may find out whether the new solutions are better, equal, or worse in any specified category than the original portfolio in use.

Assets, Vulnerabilities, Threats

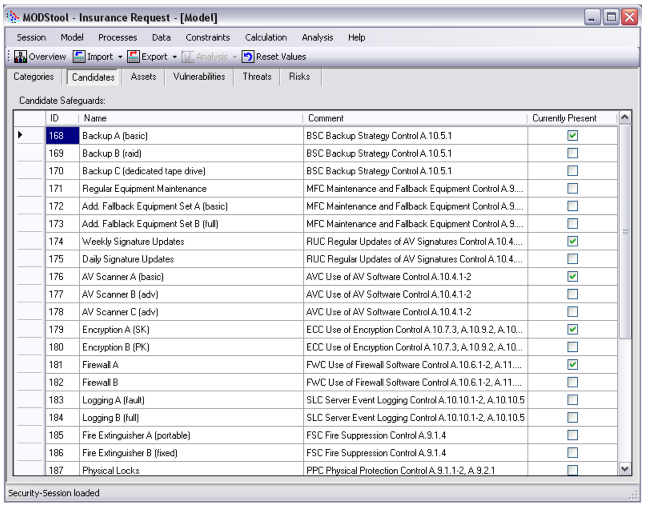
The Assets, Vulnerabilities, and Threats tabpages are constructed similarly to the Candidates page with IDs, the mandatory names, and optional comments. The threats include an additional column, their ARO (entries must be non-negative numbers). Again, the entries can be directly edited in the grid.

For assets and threats imported via XML files, their comment entries are set to their type: IT System, Machinery, Communication Device, Data, and Other for assets; Misuse and Abuse for threats.

Risks

In this tabpage, risks are composed by mapping vulnerabilities and threats to assets. The top grid allows the adding, deleting, and editing of risks. Adding a risk is done by entering a mandatory name and choosing an asset, vulnerability, and threat from the corresponding comboboxes.

Risk mappings, i.e. safeguards that counter a selected risk, can only be modified



Candidate Safeguards:

ID	Name	Comment	Currently Present
168	Backup A (basic)	BSC Backup Strategy Control A.10.5.1	☑
169	Backup B (raid)	BSC Backup Strategy Control A.10.5.1	□
170	Backup C (dedicated tape drive)	BSC Backup Strategy Control A.10.5.1	□
171	Regular Equipment Maintenance	MFC Maintenance and Fallback Equipment Control A.9....	□
172	Add. Fallback Equipment Set A (basic)	MFC Maintenance and Fallback Equipment Control A.9....	□
173	Add. Falblack Equipment Set B (full)	MFC Maintenance and Fallback Equipment Control A.9....	□
174	Weekly Signature Updates	RUC Regular Updates of AV Signatures Control A.10.4....	☑
175	Daily Signature Updates	RUC Regular Updates of AV Signatures Control A.10.4....	□
176	AV Scanner A (basic)	AVC Use of AV Software Control A.10.4.1-2	☑
177	AV Scanner B (adv)	AVC Use of AV Software Control A.10.4.1-2	□
178	AV Scanner C (adv)	AVC Use of AV Software Control A.10.4.1-2	□
179	Encryption A (SK)	ECC Use of Encryption Control A.10.7.3, A.10.9.2, A.10...	☑
180	Encryption B (PK)	ECC Use of Encryption Control A.10.7.3, A.10.9.2, A.10...	□
181	Firewall A	FWC Use of Firewall Software Control A.10.6.1-2, A.11....	☑
182	Firewall B	FWC Use of Firewall Software Control A.10.6.1-2, A.11....	□
183	Logging A (fault)	SLC Server Event Logging Control A.10.10.1-2, A.10.10.5	□
184	Logging B (full)	SLC Server Event Logging Control A.10.10.1-2, A.10.10.5	□
185	Fire Extinguisher A (portable)	FSC Fire Suppression Control A.9.1.4	□
186	Fire Extinguisher B (fixed)	FSC Fire Suppression Control A.9.1.4	□
187	Physical Locks	PPC Physical Protection Control A.9.1.1-2, A.9.2.1	□

Security-Session loaded

Figure 5.5.: Model - Candidates

(added/removed via the buttons) when the edit focus is on the mappings grid. If the focus lies on the top risk composition grid, the mapping list is displayed, but no adding of additional safeguards to or removing from the list is allowed. Switching the focus between the top risk grid and the lower right mapping grid is done by clicking on the corresponding grid. Switching focus also saves any changes made in the current grid to the database, in addition to saving when leaving the tabpage. The grid with the bold label indicates which grid is currently focused. The lower left grid displays all available safeguards specified for the current session.

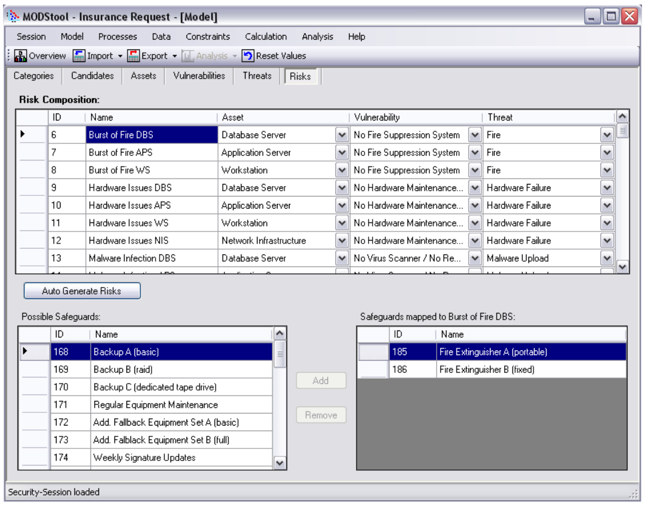
Auto Generate Risks automatically generates all possible combinations of assets, vulnerabilities, and threats, and stores them in the database, if not already inserted. In this tabpage, Reset Values reloads the values of the currently focused grid.

5.2.3. Processes

The optional process-related information is only needed if process-related categories are defined and includes the category value of the process, asset impact, and process-related safeguard effectiveness.

Asset Impact

The Asset Impact tabpage allows the input of the category value generated by the business process and the impact factor of each asset on the process value. Generated value is entered in the top grid where all process-related categories are displayed, assets and



Risk Composition:

ID	Name	Asset	Vulnerability	Threat
6	Burst of Fire DBS	Database Server	No Fire Suppression System	Fire
7	Burst of Fire APS	Application Server	No Fire Suppression System	Fire
8	Burst of Fire WS	Workstation	No Fire Suppression System	Fire
9	Hardware Issues DBS	Database Server	No Hardware Maintenance...	Hardware Failure
10	Hardware Issues APS	Application Server	No Hardware Maintenance...	Hardware Failure
11	Hardware Issues WS	Workstation	No Hardware Maintenance...	Hardware Failure
12	Hardware Issues NIS	Network Infrastructure	No Hardware Maintenance...	Hardware Failure
13	Malware Infection DBS	Database Server	No Virus Scanner / No Re...	Malware Upload

Possible Safeguards:

ID	Name
168	Backup A (basic)
169	Backup B (raid)
170	Backup C (dedicated tape drive)
171	Regular Equipment Maintenance
172	Add. Fallback Equipment Set A (basic)
173	Add. Falblack Equipment Set B (full)
174	Weekly Signature Updates

Safeguards mapped to Burst of Fire DBS:

ID	Name
185	Fire Extinguisher A (portable)
186	Fire Extinguisher B (fixed)

Security-Session loaded

Figure 5.6.: Model - Risks

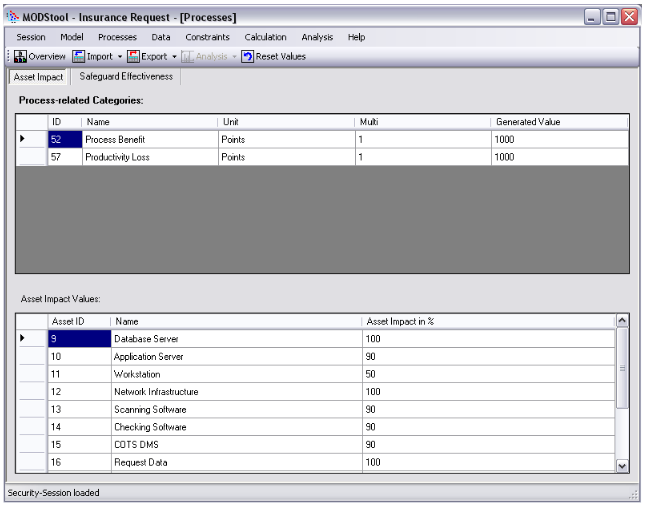
their impact values are displayed in the lower grid. Again, the edit focus is switched by clicking on the corresponding grid, and by selecting another category the corresponding asset impact values are displayed, as well as previously modified entries saved in the database. Impact values may range from 0 to 100 percent, whereas 0 defines no impact of an asset on the category at all and 100 the full impact. Note that no adding or removing of risks and assets, nor editing except for the values are allowed. Alike the Risk tabpage, the Reset Values button reloads data of the currently focused grid.

Safeguard Effectiveness

In this sub-form, the effectiveness of safeguards to protect a certain asset for processes can be specified. Technically, this tabpage is constructed similarly to the former Asset Impact page: The top grid shows all assets/safeguard mappings defined for the session, set by the risk/safeguard mappings, and the lower grid all process-related categories and corresponding safeguard effectiveness values. The only editable columns are the entries for the safeguard effectiveness expressed in percent. Note that these factors are defined independently from the safeguard effectiveness values for risk categories and express how well the safeguards can ensure the assets' availability for the processes.

5.2.4. Data

The Data function group is responsible for the input of the quantitative data for the risks and safeguards. Data input is divided into asset and vulnerability values, risk inclusion,



Process-related Categories:

ID	Name	Unit	Multi	Generated Value
52	Process Benefit	Points	1	1000
57	Productivity Loss	Points	1	1000

Asset Impact Values:

Asset ID	Name	Asset Impact in %
9	Database Server	100
10	Application Server	90
11	Workstation	50
12	Network Infrastructure	100
13	Scanning Software	90
14	Checking Software	90
15	COTS DMS	90
16	Request Data	100

Security-Session loaded

Figure 5.7.: Processes - Asset Impact

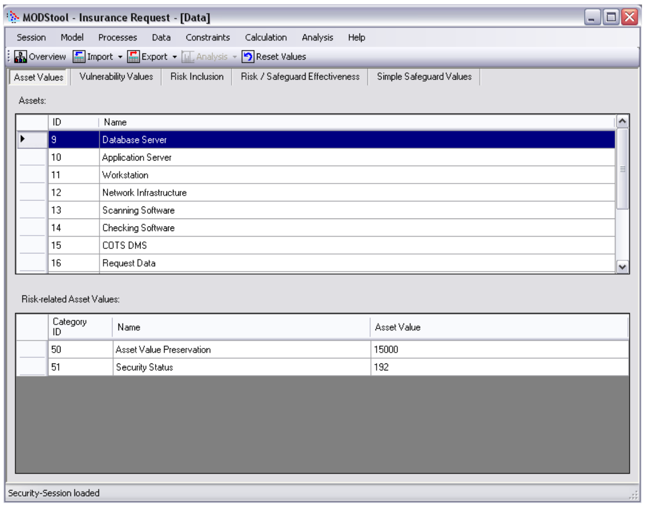
risk-related safeguard effectiveness, and the safeguard values for the remaining simple categories.

Asset and Vulnerability Values

The Asset and Vulnerability Values tabpages are responsible for handling risk-related, category dependent values. The upper grids show the assets and vulnerabilities, whereas the lower grids present the values of the selected assets and exposure factors of vulnerabilities for all risk-related categories. Vulnerability exposure factors are measured in percent. Only the values and exposure factor columns are editable. Apart from data saving when leaving the tabpages, changes are also saved when selecting another entity.

Risk Inclusion

The Risk Inclusion tabpage allows the user to explicitly include or exclude risks from the evaluation process. The whole idea of this function is to consider important risks only and to ignore negligible ones. The risk matrix is divided into three areas, representing the importance of risks: Red colored cells indicate risks with high ARO and exposure (impact) that are most pressing and should be dealt with by all means. Yellow colored cells contain risks with high exposure but a relatively low ARO, representing risks with a lower probability to occur but still having a high impact. These should be considered as well because of their serious impact on asset values. Green colored cells include risks with low to high ARO and a low impact. Those are quite negligible as their impact on



Assets:

ID	Name
9	Database Server
10	Application Server
11	Workstation
12	Network Infrastructure
13	Scanning Software
14	Checking Software
15	COTS DMS
16	Request Data

Risk-related Asset Values:

Category ID	Name	Asset Value
50	Asset Value Preservation	15000
51	Security Status	192

Security-Session loaded

Figure 5.8.: Data - Asset Values

asset value is quite low, although their probability of occurrence may be quite high. By default, all borders are set between 50 and 60 percent, but can be changed as desired by using the ARO/Exposure Offset scrollbars.

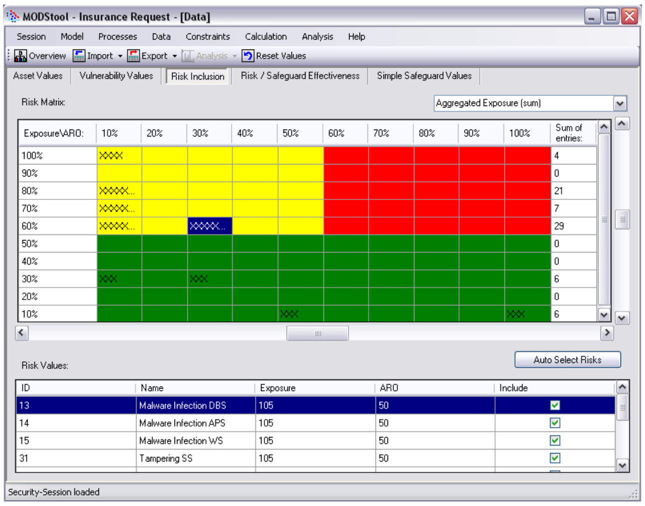
Risks are automatically inserted into their corresponding group and marked according to their relative exposure/ARO values (in percent), whereas 100 percent indicates the highest values of all risks (if the max. value of AROs of all risks is lower than 10, max. ARO is set to 10).

By selecting another (risk-related) category in the upper right combobox, the risks are inserted into the matrix according to their category exposure factors. Aggregated Exposure indicates the simple sum of all category specific exposure factors for each safeguard and is the default.

An X indicates that the specific risk is currently marked as included, an O otherwise. The lower grid displays information about all risks of the currently selected group (risk matrix cell); exposure factors correspond to the selected category. By checking/unchecking the Include checkbox, the user can manually change the inclusion mark of each risk. Additionally, the Auto Select Risks function automatically marks all risks in yellow and red cells to be included.

Risk/Safeguard Effectiveness

The Risk/Safeguard Effectiveness tabpage allows the input of the effectiveness values for each specified risk/safeguard mapping. In the top grid, mappings are selected and their corresponding safeguard effectiveness values are displayed in the lower grid. Effectiveness



Risk Matrix: Aggregated Exposure (sum)

Exposure\ARO:	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%	Sum of entries:
100%	🟨 XXXX	🟨	🟨	🟨	🟨	🟥	🟥	🟥	🟥	🟥	4
90%	🟨	🟨	🟨	🟨	🟨	🟥	🟥	🟥	🟥	🟥	0
80%	🟨 XXXXX...	🟨	🟨	🟨	🟨	🟥	🟥	🟥	🟥	🟥	21
70%	🟨 XXXXX...	🟨	🟨	🟨	🟨	🟥	🟥	🟥	🟥	🟥	7
60%	🟨 XXXXX...	🟨	XXXXX...	🟨	🟨	🟥	🟥	🟥	🟥	🟥	29
50%	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	0
40%	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	0
30%	🟩 XXX	🟩	🟩 XXX	🟩	🟩	🟩	🟩	🟩	🟩	🟩	6
20%	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	0
10%	🟩	🟩	🟩	🟩	🟩 XXX	🟩	🟩	🟩	🟩	🟩 XXX	6

Risk Values:

ID	Name	Exposure	ARO	Include
13	Malware Infection DBS	105	50	☑
14	Malware Infection APS	105	50	☑
15	Malware Infection WS	105	50	☑
31	Tampering SS	105	50	☑

Security-Session loaded

Figure 5.9.: Data - Risk Inclusion

values are not set for each safeguard, but for each risk/safeguard mapping (safeguards may be more/less effective in countering a certain risk than another one). Effectiveness is set for each risk-related category independently.

Simple Safeguard Values

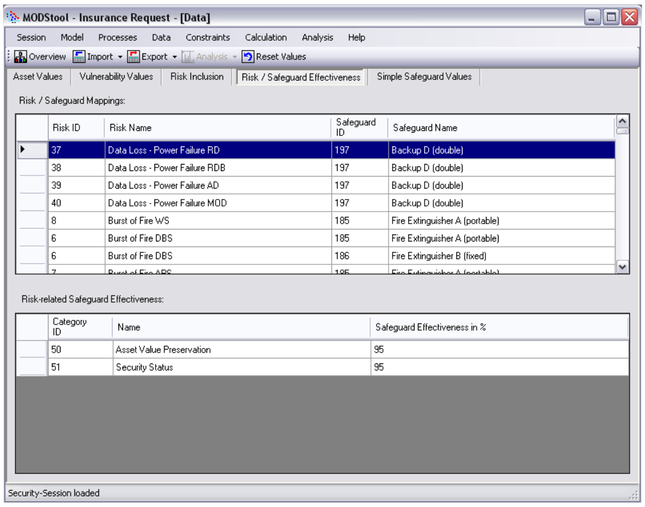
In the last of the Data-related tabpages, values for all simple categories are entered. The upper grid displays all safeguards, while the values for each simple category can be entered in the lower grid.

5.2.5. Constraints

The Constraint sub-form is responsible for handling all constraints including upper and lower borders of category values, inclusion and exclusion constraints, and synergy and cannibalism relations.

Category Limits

Category limits specify the upper and lower borders for aggregated category values: For benefit categories, the limits define the minimum value that have to be reached by the safeguard portfolio in order to be valid. For resource categories, the limits define the maximum value that must not be exceeded. The constraints are set for the selected aggregation type of the categories.



Risk / Safeguard Mappings:

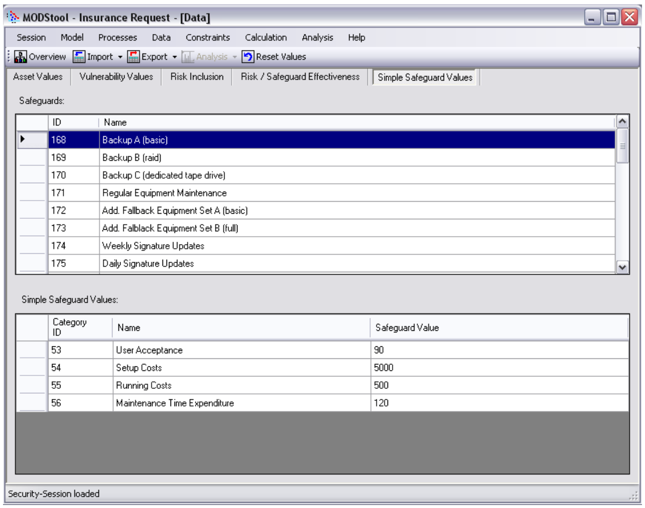
Risk ID	Risk Name	Safeguard ID	Safeguard Name
37	Data Loss - Power Failure RD	197	Backup D (double)
38	Data Loss - Power Failure RDB	197	Backup D (double)
39	Data Loss - Power Failure AD	197	Backup D (double)
40	Data Loss - Power Failure MOD	197	Backup D (double)
8	Burst of Fire WS	185	Fire Extinguisher A (portable)
6	Burst of Fire DBS	185	Fire Extinguisher A (portable)
6	Burst of Fire DBS	186	Fire Extinguisher B (fixed)
7	Burst of Fire ABS	185	Fire Extinguisher A (portable)

Risk-related Safeguard Effectiveness:

Category ID	Name	Safeguard Effectiveness in %
50	Asset Value Preservation	95
51	Security Status	95

Security-Session loaded

Figure 5.10.: Data - Risk/Safeguard Effectiveness



Safeguards:

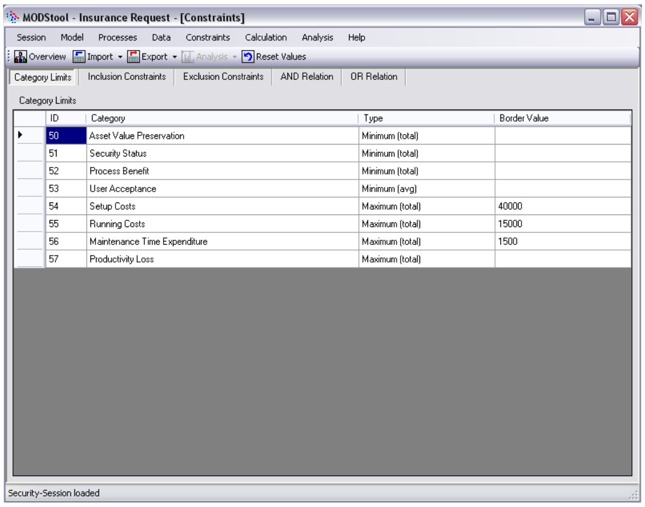
ID	Name
168	Backup A (basic)
169	Backup B (raid)
170	Backup C (dedicated tape drive)
171	Regular Equipment Maintenance
172	Add. Fallback Equipment Set A (basic)
173	Add. Falblack Equipment Set B (full)
174	Weekly Signature Updates
175	Daily Signature Updates

Simple Safeguard Values:

Category ID	Name	Safeguard Value
53	User Acceptance	90
54	Setup Costs	5000
55	Running Costs	500
56	Maintenance Time Expenditure	120

Security-Session loaded

Figure 5.11.: Data - Simple Safeguard Values



Category Limits

ID	Category	Type	Border Value
50	Asset Value Preservation	Minimum (total)	
51	Security Status	Minimum (total)	
52	Process Benefit	Minimum (total)	
53	User Acceptance	Minimum (avg)	
54	Setup Costs	Maximum (total)	40000
55	Running Costs	Maximum (total)	15000
56	Maintenance Time Expenditure	Maximum (total)	1500
57	Productivity Loss	Maximum (total)	

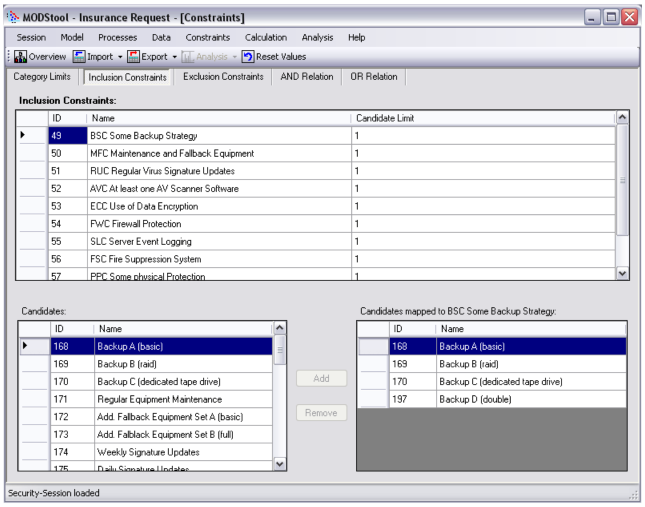
Figure 5.12.: Constraints - Category Limits

Inclusion and Exclusion Constraints

Inclusion and exclusion constraints define constraints regarding the number of certain safeguards included in the solutions. Inclusion refers to the minimum number of safeguards out of a specified list that has to be included in the solution to be valid. Exclusion refers to the maximum number of safeguards that is allowed. The list can be created and altered for each constraint independently by using the Add and Remove buttons. Focus is changed by clicking on the top constraint grid and the lower right mapping grid (cf. Risks).

AND and OR Relations

The AND and OR relations handle the definition of synergy and cannibalism effects that occur when a specified number of safeguards out of a defined list is included in the portfolio. AND relations represent the minimum number of included safeguards necessary for the effects to be triggered, OR relations the maximum number. Technically, relations are very similar to constraints, but a safeguard combination that does not meet one relation is not regarded as invalid but just does not trigger the either positive or negative effect on a category value. The relation grid also allows the choice of the affected category by selecting the appropriate combobox item and the input of the corresponding value.



Inclusion Constraints:

ID	Name	Candidate Limit
49	BSC Some Backup Strategy	1
50	MFC Maintenance and Fallback Equipment	1
51	RUC Regular Virus Signature Updates	1
52	AVC At least one AV Scanner Software	1
53	ECC Use of Data Encryption	1
54	FWC Firewall Protection	1
55	SLC Server Event Logging	1
56	FSC Fire Suppression System	1
57	PPC Some physical Protection	1

Candidates:

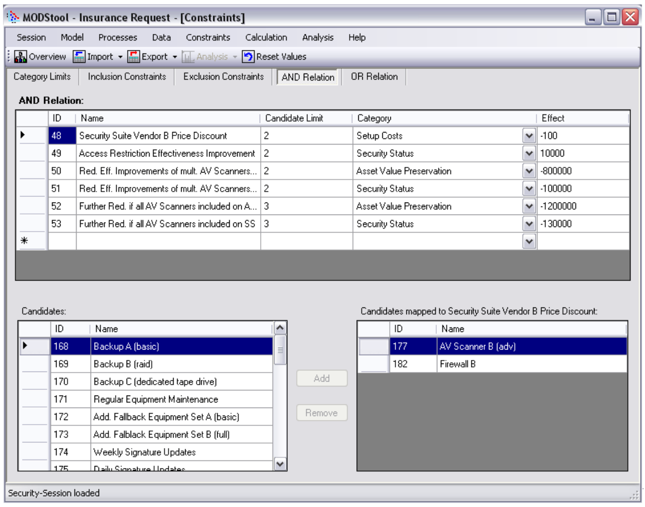
ID	Name
168	Backup A (basic)
169	Backup B (raid)
170	Backup C (dedicated tape drive)
171	Regular Equipment Maintenance
172	Add. Fallback Equipment Set A (basic)
173	Add. Falblack Equipment Set B (full)
174	Weekly Signature Updates
175	Daily Signature Updates

Candidates mapped to BSC Some Backup Strategy:

ID	Name
168	Backup A (basic)
169	Backup B (raid)
170	Backup C (dedicated tape drive)
197	Backup D (double)

Security-Session loaded

Figure 5.13.: Constraints - Inclusion Constraints



AND Relation:

ID	Name	Candidate Limit	Category	Effect
48	Security Suite Vendor B Price Discount	2	Setup Costs	-100
49	Access Restriction Effectiveness Improvement	2	Security Status	10000
50	Red. Eff. Improvements of mult. AV Scanners...	2	Asset Value Preservation	-800000
51	Red. Eff. Improvements of mult. AV Scanners...	2	Security Status	-100000
52	Further Red. if all AV Scanners included on A...	3	Asset Value Preservation	-1200000
53	Further Red. if all AV Scanners included on SS	3	Security Status	-130000

Candidates:

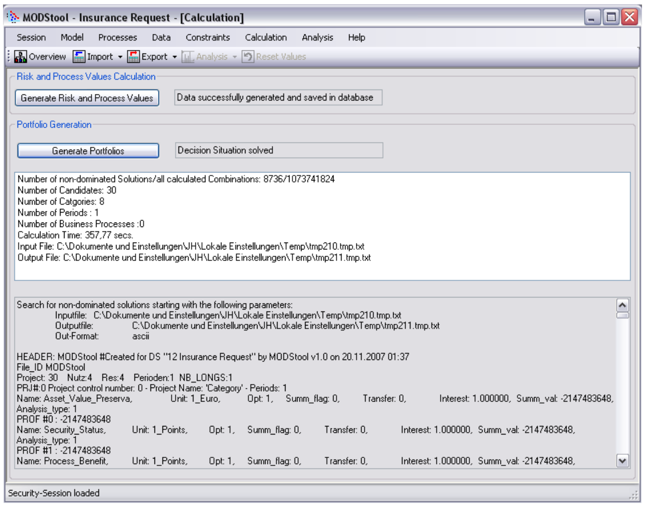
ID	Name
168	Backup A (basic)
169	Backup B (raid)
170	Backup C (dedicated tape drive)
171	Regular Equipment Maintenance
172	Add. Fallback Equipment Set A (basic)
173	Add. Falblack Equipment Set B (full)
174	Weekly Signature Updates
175	Daily Signature Updates

Candidates mapped to Security Suite Vendor B Price Discount:

ID	Name
177	AV Scanner B (adv)
182	Firewall B

Security-Session loaded

Figure 5.14.: Constraints - And Relations



Data successfully generated and saved in database

Decision Situation solved

```
Number of non-dominated Solutions/all calculated Combinations: 8736/1073741824
Number of Candidates: 30
Number of Catgories: 8
Number of Periods : 1
Number of Business Processes :0
Calculation Time: 357,77 secs.
Input File: C:\Dokumente und Einstellungen\JH\Lokale Einstellungen\Temp\tmp210.tmp.txt
Output File: C:\Dokumente und Einstellungen\JH\Lokale Einstellungen\Temp\tmp211.tmp.txt
```

```
Search for non-dominated solutions starting with the following parameters:
        Inputfile:   C:\Dokumente und Einstellungen\JH\Lokale Einstellungen\Temp\tmp210.tmp.txt
        Outputfile:         C:\Dokumente und Einstellungen\JH\Lokale Einstellungen\Temp\tmp211.tmp.txt
        Out-Format:         ascii

HEADER: MODStool #Created for DS "12 Insurance Request" by MODStool v1.0 on 20.11.2007 01:37
File_ID MODStool
Project: 30   Nutz:4   Res:4   Perioden:1  NB_LONGS:1
PRJ#:0 Project control number: 0 - Project Name: 'Category' - Periods: 1
Name: Asset_Value_Preserva,        Unit: 1_Euro,      Opt: 1,    Summ_flag: 0,      Transfer: 0,        Interest: 1.000000,  Summ_val: -2147483648,
Analysis_type: 1
PROF #0 : -2147483648
Name: Security_Status,      Unit: 1_Points,     Opt: 1,    Summ_flag: 0,      Transfer: 0,        Interest: 1.000000,  Summ_val: -2147483648,
Analysis_type: 1
PROF #1 : -2147483648
Name: Process_Benefit,      Unit: 1_Points,     Opt: 1,    Summ_flag: 0,      Transfer: 0,        Interest: 1.000000,  Summ_val: -2147483648,
```

Security-Session loaded

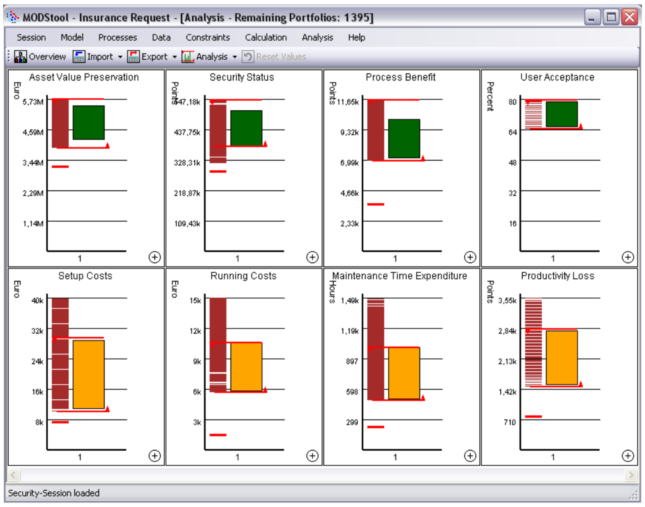
Figure 5.15.: Calculation

5.2.6. Calculation

The Calculation screen provides functions to determine all non-dominated portfolios. The upper button is used for the calculation and storage of risk- and process-related safeguard values prior to the search process. The lower button is only accessible when the risk/process value generation was successful and initiates the portfolio generation: At first, the currently deployed security situation is determined by calculating the category values of safeguards marked as currently in use and is stored in the database. Then, data for the optimization process is fetched from the database and written into an ASCII-encoded input file and the INNOV process started. Upon completion of the evaluation process, the results are written to the output file and finally saved in the database. The center box of the Calculation sub-form provides statistics including the number of non-dominated portfolios and the total number of candidates and categories. The lower box displays the INNOV input data for verification. The small textboxes provide feedback whether the generation of the risk/process values and the generation of non-dominated portfolios were successful. During the calculation process, the estimated and elapsed times are displayed. The calculation can be aborted with the button.

5.2.7. Analysis

The Analysis sub-form is actually the embedded main form of the ATANA framework and is instantiated when the corresponding menuitem is selected. The Analysis drop-down menu in the toolstrip is enabled then. The values of the non-dominated portfolios



MODStool - Insurance Request - [Analysis - Remaining Portfolios: 1395]

Security-Session loaded

Figure 5.16.: Analysis

are displayed as vertical bars in their respective benefit and resource categories. By moving the red horizontal bars up and down, tighter restrictions can be imposed on the solutions, thus reducing the number of remaining valid combinations. Thereby, a more manageable number of solutions can be examined more thoroughly. On the left of the bars, brown lines represent the individual category values of all portfolios. The green line indicates the value of the currently deployed safeguard portfolio for comparison. If this value exceeds/drops below the maximum/minimum value of all other new combinations, this line is colored red instead.

5.2.8. Help

The Help menuitem in the menustrip allows access to the Online help and 'About' information of the tool with the usual entries Contents, Index, and About.

5.2.9. Overview

The Overview function found in the toolstrip displays a navigational help in the form of a diagram, explaining the coherences between the tabpages and the general workflow. All tabpages are represented by a red label that are colored green if visited and directly link to their corresponding pages. The button on the lower right resets all links to red.

5.2.10. Import

The Import item allows access to import functions that are divided into the following two: XML and Other Sessions. Importable entities are as follows:

XML Assets and threats from Adonis generated XML (only entities); Categories, Assets, Vulnerabilities, Threats, Safeguards, Risks, Constraints, Relations, or all at once from MODStool generated XML (with existing quantitative valuations).

Other Sessions All entities with any corresponding quantitative valuations.

XML importable entities are added by selecting the XML file containing them in the file dialog. After clicking on the open button, all new entities (i.e. those that are not included in the current session yet) are inserted into the database and the corresponding tabpage is shown.

Entities imported from other sessions are added by selecting the desired entries out of the list in the opened grid and accepting the selection. Again, only new entities are added and the corresponding tabpage is shown.

To determine whether a certain entity is not yet specified for the current session, its name is compared to all others of the same entity type; for categories, their different category types (benefit or resource and risk/process/simple) are considered too, as well as type for Constraints (Inclusion or Exclusion) and Relations (And or Or). Quantitative data is only added if related entities are existing, e.g. when importing assets, their values are added only if their related categories are existing for the particular session. Process-related effectiveness values of safeguards are exported/imported automatically with risk (mappings).

Apart from these entities, analysis data (non-dominated portfolios and category limitations) can be imported too, when the Analysis form is active.

5.2.11. Export

The Export item allows exporting entities and their quantitative valuations to XML files to be imported to other sessions, as well as analysis data.

5.2.12. Analysis

The Analysis item provides access to Analysis specific forms and functions including category selection, portfolio selection, and detailed portfolio information.

5.3. Architecture

5.3.1. Overview

The classes of the MODStool framework can be divided into three categories:

Form Classes The form classes generate the graphic user interface. It is their responsibility to provide data presentation and mechanisms for data manipulation. The main form serves as the container for the sub-forms that represent the functional groups. The sub-forms, in turn, serve as the containers for the tabpages which provide the individual functions.

Handler Classes The handler classes are called from the form classes and handle all data access functions. They are responsible for connecting to the database, fetching the data and providing the form classes with filled data sets, and for updating the data tables in the database with the changes made in the forms by the user.

Miscellaneous Classes The remaining classes provide helper functions for certain tasks and other classes, e.g. AdonisImporter class for importing assets and threats from Adonis generated XML-files.

5.3.2. Form Classes

MainForm The main 'window' for this application hosts the subforms once a session has been loaded. NewSession and OpenSession can be accessed from here. Invokes the NewSessionForm, OpenSessionForm, ModelFormSec, ProcessesFormSec, DataFormSec, ConstraintsForm, AnalysisForm, ImportEntitiesForm, OverviewForm, AboutForm, Splash, and AdonisImporter classes.

OpenSessionForm Dialog for opening an existing session (copy and original). Invokes the SessionHandler class.

NewSessionForm Dialog for creating a new session. Invokes the SessionHandler class.

ModelFormSec Displays the model specific information and allows the manipulation of benefit and resource categories, candidate safeguards, assets, threats, vulnerabilities, and risks. Invokes the ImportCandidatesForm, CategoryHandler, CandidateHandler, AssetHandler, VulnerabilityHandler, ThreatHandler, and RiskHandler classes.

ProcessesFormSec Allows the input and modification of process-related quantitative data. Invokes the CategoryHandler and AssetHandler classes.

DataFormSec Displays quantitative data of risks and safeguards and allows their modification. Invokes AssetHandler, VulnerabilityHandler, RiskHandler, and CandidateValuesHandler classes.

ConstraintsForm Handles all constraints and interdependencies including category limits, inclusion/exclusion constraints, and AND/OR relations. Invokes CategoryLimitsHandler, ConstraintHandler, ConstraintMappingHandler, RelationHandler, and RelationMappingHandler classes.

CalculationForm Serves as interface to the INNOV library and provides feedback of the portfolio generation process. Invokes the Solver and Progress classes.

AnalysisForm Actually the embedded ATANA main screen. Invokes its own specific classes.

OverviewFormSec Shows the navigational overview diagram.

ImportEntitiesForm Dialog for selecting entities (categories, safeguards, assets, vulnerabilities, threats, risks, constraints, relations) to be imported from other sessions. Invokes CategoryHandler, CandidateHandler, AssetHandler, VulnerabilityHandler, and ThreatHandler classes.

RenameSessionForm Allows renaming the currently loaded session.

ConfirmDeletionForm Asks for confirmation to delete the selected session.

Splash Realizes the splash screen shown at the startup of the application.

Progress Creates a simple progressbar displayed during the calculation of the non-dominated solutions including the elapsed and estimated times and the button for aborting the calculation.

AboutForm Displays the About-information of the tool.

5.3.3. Handler Classes

SessionHandler Handles the database functions for sessions.

CategoryHandler Handles the database functions for the benefit and resource categories.

CandidateHandler Handles the database functions for the candidate safeguards.

CandidateValuesHandler Handles the database functions for category dependent safeguard values.

AssetHandler Handles the database functions for assets.

VulnerabilityHandler Handles the database functions for vulnerabilities.

ThreatHandler Handles the database functions for threats.

RiskHandler Handles the database functions for the composed risks.

CategoryLimitsHandler Handles the database functions for the category limits.

ConstraitsHandler Handles the database functions for inclusion and exclusion constraints.

ConstraintsMappingHandler Handles the database functions for the candidate/ constraint mappings.

RelationHandler Handles the database functions for AND and OR relations.

RelationMappingHandler Handles the database functions for the candidate/relation mappings.

SolutionHandler Handles the database functions for the non-dominated solutions and contains other utility functions.

5.3.4. Miscellaneous Classes

Program Entry point for the application. Invokes the MainForm class.

XMLImporter Responsible for importing data from XML-files generated by the Adonis tool or MODStool including parsing the files and saving the data in the database. Invokes all handler classes except SessionHandler and SolutionHandler.

XMLExporter Responsible for writing MODStool entity data (including values) to XML files. Invokes all handler classes except SessionHandler and SolutionHandler.

Solver The solver class functions as the interface class between the MODStool framework and the INNOV tool. It is responsible for generating the risk/process-related values and for the update of the safeguard values in the database, as well as the calculation of category values of currently present safeguards. It also generates the input file, starts the optimization process and stores the solutions of the output file in the database for the ATANA visualization. Invokes the SolutionHandler, CategoryHandler, CandidateHandler, CandidateValuesHandler, AssetHandler, RiskHandler, EvaluationResult, ProcessCat, PresentCandidatesValues, RiskŽ, and Safeguard classes.

EvaluationResult Represents the data structure for the solutions. Used for saving the results in the database.

ProcessCat Represents the data structure for process-related categories. Used for the calculation of process-related safeguard values.

Risk Represents the data structure for risks. Used for the calculation of risk-related safeguard values.

Safeguard Represents the data structure for safeguards. Used for the calculation of risk/process-related safeguard values.

PresentCandidatesValues Represents the data structure for category values of currently present and deployed safeguards.

ErrorHandler Although a handler class by name, the ErrorHandler does not belong to this group, as it does not handle any data access functions. It contains general error messages and can be invoked by the other classes.

CopyHelper Contains methods to copy a whole session (except for any solution data) and saves it to the database. Invokes all other handler classes except SolutionHandler.

5.4. Data Model

One of the requirements of the tool is the permanent storage of data in a relational database. There are six main data table groups, roughly representing the different functions provided by the tool:

5.4.1. Session

The Session group consists only of the DecisionSituation table. This is where all the session information is stored including the ID, description, and session type. All other entities are either directly (via foreign key) or indirectly related to a DecisionSituation data entry.

5.4.2. General

The General group contains all data tables that are not exclusive to one of the other groups but are referenced by multiple other entities.

Candidates Stores candidate safeguard information.

Category Stores category data including description and type, but also the generated utility value in case of a process-related category.

CandidateCategory Stores the mapping of safeguards to categories.

PeriodValue Stores different types of quantitative data including safeguard values for different categories, category limits, and synergy/cannibalism effects.

5.4.3. Risk

This larger group contains all entities that are directly related to risks including asset, vulnerability, and threat information, as well as mappings.

Asset Stores asset information.

Vulnerability Stores information about vulnerabilities.

Threat Stores threat information including their AROs.

Risks Stores asset, vulnerability, and threat mappings.

CandidateRisks Stores safeguards assigned to risks in terms of foreign key pairs.

CandidateRiskCategory Stores the effectiveness values of safeguards for each risk and risk-related category.

AssetCategory Stores asset values for each risk category and asset impact values for process-related categories.

VulnerabilityCategory Stores the vulnerabilities' exposure factors for each risk-related category.

5.4.4. Process

The two members of this group are responsible for storing process-related data:

AssetCandidate Stores asset/candidate mappings, that are set automatically when risk mappings are defined. If a certain asset/candidate mapping is already set, no duplicates are inserted, e.g. if safeguards are mapped to the same asset multiple times by being assigned to multiple risks.

AssetCandidateCategory Stores effectiveness values for each asset/candidate mapping and process-related category. Impact values of assets are stored in the AssetCategory data table.

5.4.5. Constraint

The Constraint group encompasses all data tables responsible for storing constraints and interdependencies. Category limits are stored in the PeriodValue data table.

Constraint Stores both inclusion and exclusion constraints.

ConstraintCandidate Stores the mappings of candidate safeguards to constraints.

Relation Stores both AND and OR relations. Synergy and cannibalism effects are stored in the PeriodValue entity.

RelationCandidate Stores the mappings of candidate safeguards to relations.

5.4.6. Solution

Data tables of the Solution group store valid non-dominated solutions (portfolios) of safeguards.

SOL_Portfolio Stores the solutions for the session.

SOL_PortfolioCategory Stores the solutions' aggregated value for each category.

SOL_PortfolioCandidate Stores the safeguards that are part of a portfolio.

SOL_Present Stores the category values of currently implemented safeguards.

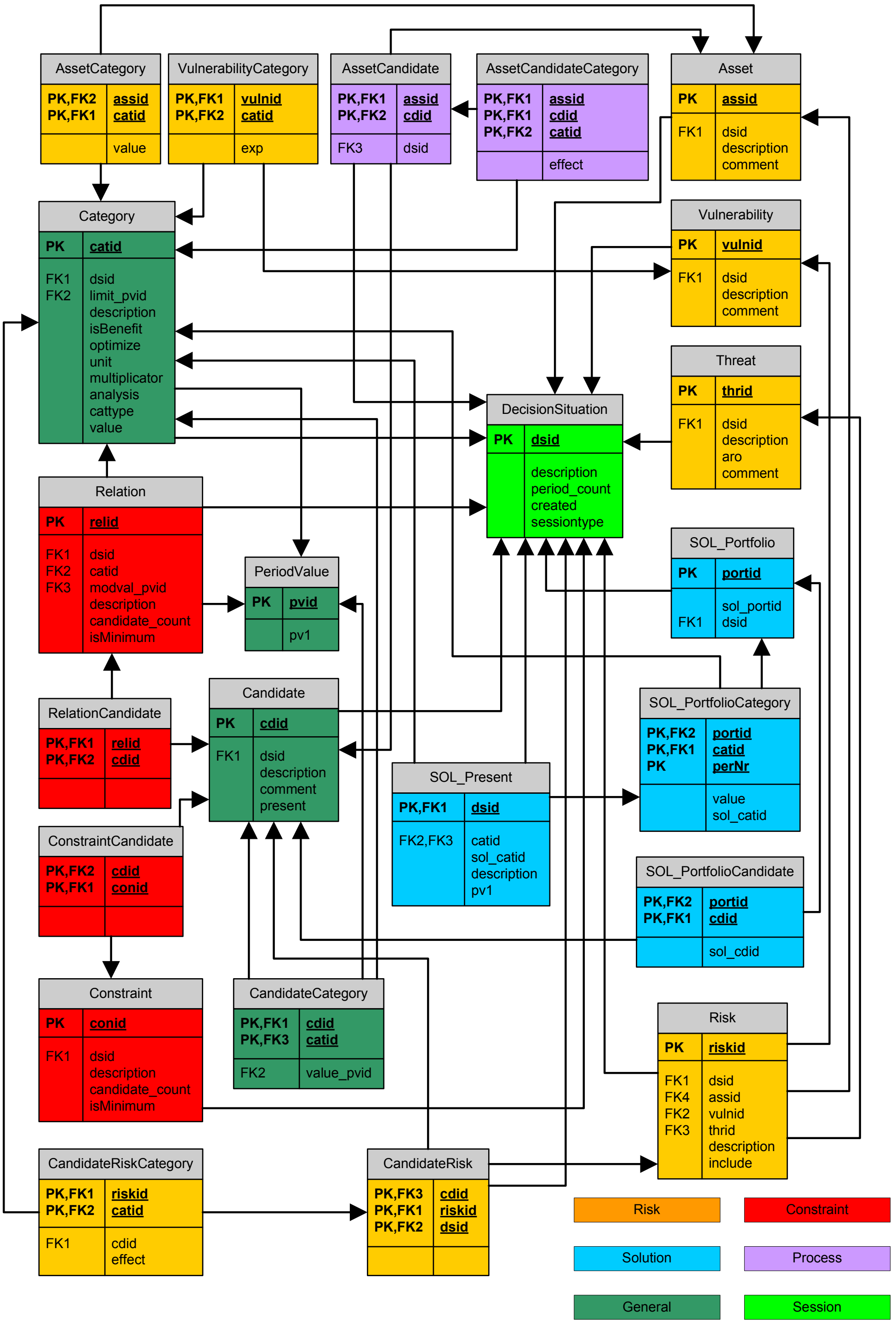


Figure 5.17.: Database Diagram

6. Application of the Proposed Framework

In this chapter, the MR-MOD is demonstrated on an exemplary accounting process of an insurance claim. The evaluation is conducted applying all three phases of the MR-MOD methodology and with the support of the MODStool software. The process workflow describes how an insurance request is checked for validity and processed within the accounting department of an insurance company.

6.1. Scenario

The business process begins with the receipt of an insurance request. At first, the request is registered by the preparer and checked for eligibility by examining the applicant's insurance status data. If the request is not eligible, it is returned to the applicant via E-Mail and the workflow ends. Otherwise, the request is scanned and the request database searched for identical requests. If an identical claim exists, the request is returned to the applicant and the workflow ends. If the request is unique and valid, the workflow continues and the assistant processes the documents. Upon completion, the request is marked for approval. Should an approval be necessary, the supervisor opens the documents of the request and inspects them. If the supervisor does not approve, the documents are edited by the assistant, before they are checked for correctness and the applicant is informed through E-Mail. Finally, a money order is send to the bank via an external web service, and the business process is completed.

The evaluation scenario of this business process is as follows:

Initial Situation No complete risk assessment has been conducted previously, but a rudimentary portfolio of safeguards is already in place. Therefore, the safeguard portfolio is not optimally arranged to suit the security requirements of that particular process.

MR-MOD Participants The following persons participate in the security evaluation: Members of the management department (specify resource limits and other organizational issues), domain expert or process owner (has process specific knowledge), and IT/security experts (provide IT- and security-related input).

Goals The aim of the evaluation process is to reach the following goals:

- Analyze the process and identify any possible risks the process is exposed to.
- Evaluate available safeguards for their effectiveness and resource requirements.
- Generate efficient safeguard portfolios and compare them to the present one.

6.2. Phase 1

Phase 1 commences with the process modeling step, where the domain expert creates a diagram of the business process and adds assets participating in the process. 16 assets of the IT System (10), Communication Device (1), Data (4) and Other (1) types are identified (fig. 6.2). Next, an IT/sec expert checks the model and analyzes the identified assets for any vulnerability; 11 vulnerabilities are specified. Then, the domain and IT/sec expert together identify and model any threats that may occur, whereas the domain expert focuses on Misuse Cases and the security expert on Abuse Cases. In total, 14 different threats are defined (6 Misuses and 8 Abuses, fig. 6.1). Finally, an initial list of 20 suitable safeguards (presently implemented and new candidates) is identified and the first phase of MR-MOD is completed.

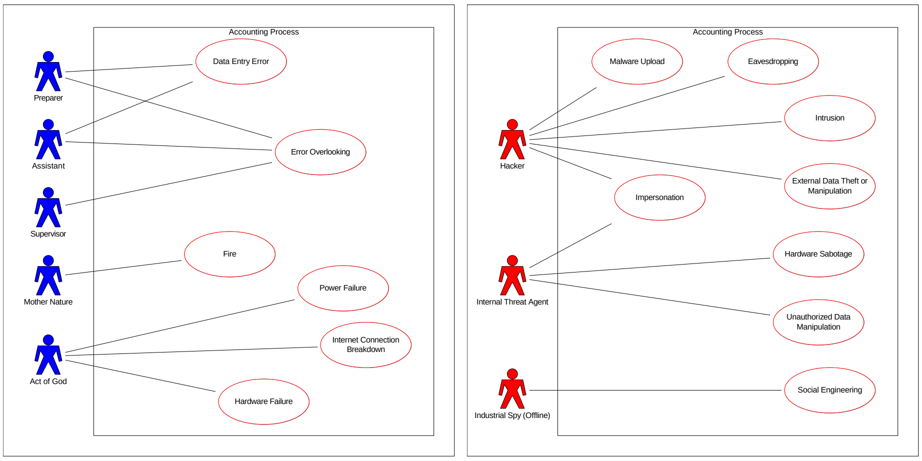


Figure 6.1.: Misuse and Abuse Case Diagrams

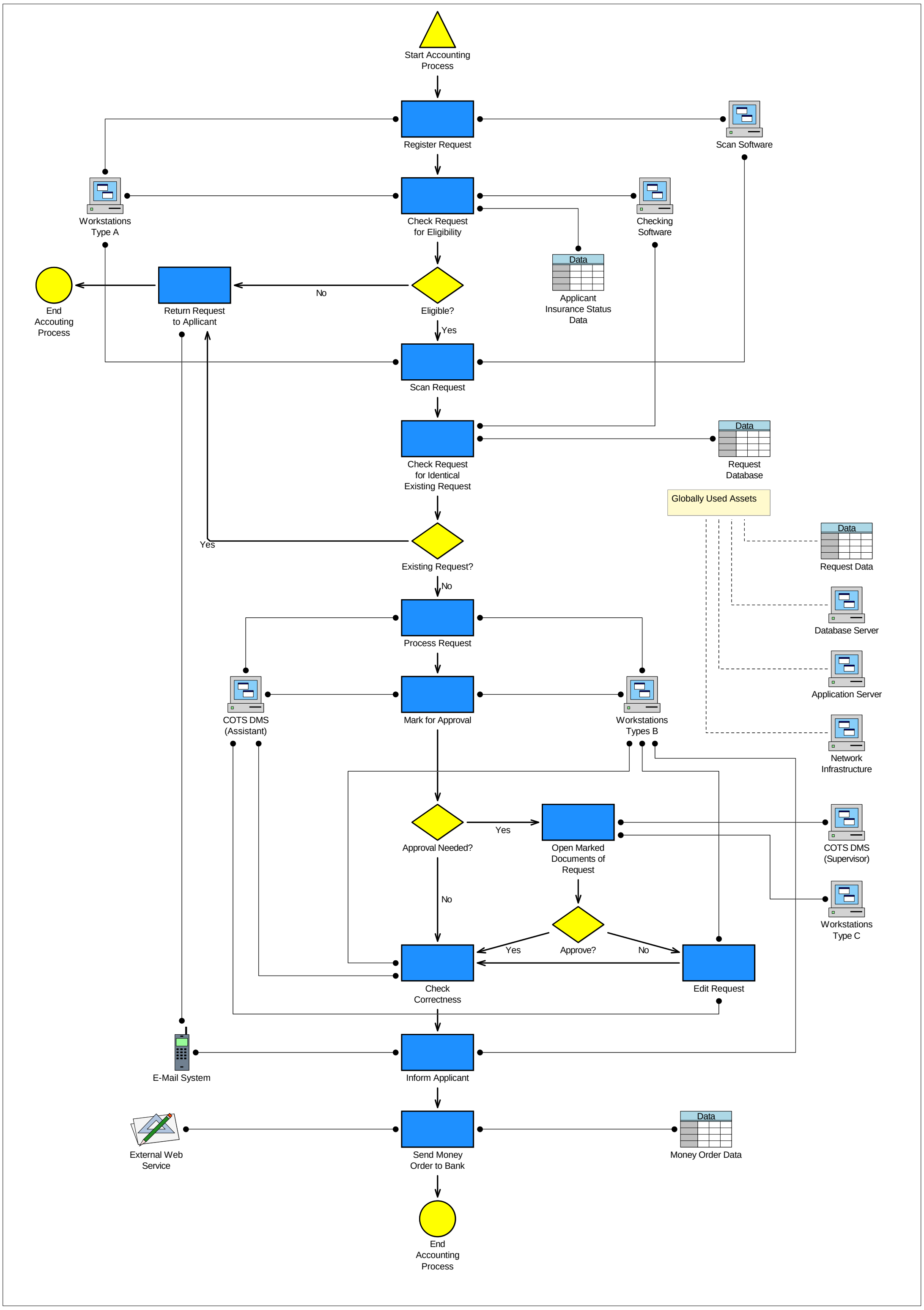


Figure 6.2.: Process Model with Assets

6.3. Phase 2

Upon completion of phase 1, the risk assessment workshop begins with members of the upper and lower management, the domain expert, IT and security specialists (network and database administrators, etc.), and system users as participants. At first, the asset, vulnerability, and threat listings are reviewed and revised, resulting in some minor changes (e.g. workstations are aggregated into one asset being technically identical). Additionally, the safeguard list is extended to 30 items according to the ISO 27001 standard[1], and the items are categorized into the following:

Technical Technical safeguards refer to IT-related technical mechanisms such as a firewalls or data encryption.

Physical Physical safeguards represent physical and non-IT-related mechanisms such as physical locks or fire extinguishers.

Operational Operational safeguards refer to introducing or improving operational procedures such as conducting regular backups.

Organizational Organizational safeguards are other methods of risk mitigation by introducing or improving present organizational matters such as introducing security training sessions for employees.

The list of all risk components is presented in table 6.1, 6.2, 6.3, and 6.4. Safeguards already in place and in use are marked with an * in list 6.4; this initial portfolio is compared to the newly generated portfolios in phase 3.

Table 6.1.: Asset List

Assets			
IT System	**Data**	**Communication**	**Other**
Database Server	Request Data	E-Mail System	External Web Service
Application Server	Request Database		
Workstation	Insurance Status Data		
Network Infrastructure	Money Order Data		
Scanning Software			
Checking Software			
COTS DMS			

[1] ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements. Only a fraction of all controls is considered in this case study.

Table 6.2.: Vulnerability List

Vulnerabilities	
No proper Backup Strategy	Lack of Security Awareness / IT Training
No Network Protection	No Virus Scanner / No Regular Updates
Lack of Encryption Techniques	No Regular Hardware Maintenance / Fallback Equipment
No proper Access Restriction Policy	No Fire Suppression Control
No or Insufficient Logging	Lack of physical Protection Mechanisms
Carelessness	

Table 6.3.: Threat List

Threats	
Misuse	**Abuse**
Data Entry Error	Malware Upload
Error Overlooking	Eavesdropping
Fire	Intrusion
Power Failure	External Data Theft or Manipulation
Internet Connection Breakdown	Impersonation
Hardware Failure	Hardware Sabotage
	Unauthorized Data Manipulation
	Social Engineering

After reviewing the lists, the workshop participants begin to identify specific risks by generating asset/vulnerability/threat-tuples: They iterate through all possible combinations of assigning vulnerabilities and threats to assets and keep plausible tuples e.g. the asset 'network infrastructure' is exposed to the threat 'eavesdropping' because of the vulnerability 'no network protection'. All non-applicable tuples, e.g. a publicly available asset 'COTS document management system' being exposed to 'social engineering' due to 'no fire suppression control', are dropped and ignored hereafter. In total, the participants agree on 73 different applicable risk combinations, and control groups are assigned to each risk then.

In the next step, the following categories are specified to measure and compare the safeguards' benefits:

Asset Value Preservation (risk) The most important goal of the evaluation process is to measure the effectiveness of safeguards to preserve the assets' value, which is measured in monetary terms. Tangible assets are valued by their replacement costs, whereas intangible assets are valued according to their business impact (or rather the business impact resulting from their compromise).

Security Status (risk) Apart from monetary asset value, another aspect of safeguards regarded as important is their effectiveness to keep the security status of assets,

Table 6.4.: Safeguard List

Safeguards		
Name	**Type**	**ISO 27001 Compliance**
BSC Backup Strategy Control		
Backup A (basic)*	Operational	A.10.5.1
Backup B (raid)	Operational	A.10.5.1
Backup C (tape drive)	Operational	A.10.5.1
Backup D (double)	Operational	A.10.5.1
MFC Maintenance/Fallback Equip. Control		
Regular Equipment Maintenance	Operational	A.9.2.4, A.14.1.1-5
Add. Fallback Equipment Set A (basic)	Operational	A.9.2.4, A.14.1.1-5
Add. Fallback Equipment Set B (full)	Operational	A.9.2.4, A.14.1.1-5
RUC Regular Updates of AV SW Control		
Virus Signature Updates A (weekly)*	Operational	A.10.4.1-2, A.12.6.1
Virus Signature Updates B (daily)	Operational	A.10.4.1-2, A.12.6.1
AVC Use Of AV Software Control		
AV Scanner A (basic)*	Technical	A.10.4.1-2
AV Scanner B (prop.)	Technical	A.10.4.1-2
AV Scanner C (prop.)	Technical	A.10.4.1-2
ECC Use Of Encryption Control		
Encryption A (SK)	Technical	A.10.7.3, A.10.9.2, A.10.10.3
Encryption B (PK)	Technical	A.10.7.3, A.10.9.2, A.10.10.3
FWC Use Of Firewall Software Control		
Firewall A*	Technical	A.10.6.1-2, A.11.4.6
Firewall B	Technical	A.10.6.1-2, A.11.4.6
Firewall C	Technical	A.10.6.1-2, A.11.4.6
Firewall D	Technical	A.10.6.1-2, A.11.4.6
Firewall E	Technical	A.10.6.1-2, A.11.4.6
SLC Server Event Logging Control		
Logging A (fault)	Technical	A.10.10.1-2, A.10.10.5
Logging B (full)	Technical	A.10.10.1-2, A.10.10.5
FSC Fire Suppression Control		
Fire Extinguisher A (portable)	Physical	A.9.1.4
Fire Extinguisher B (fixed)	Physical	A.9.1.4
PPC Physical Protection Control		
Physical Locks	Physical	A.9.1.1-2, A.9.2.1
Surveillance System	Physical	A.9.1.1-2, A.9.2.1
Security Guards	Physical	A.9.1.1-2, A.9.2.1
ETC Employee Training Control		
IT and Security Awareness Training A (basic)	Organ.	A.8.2.2
IT and Security Awareness Training B (extensive)	Organ.	A.8.2.2
ACC Access Rights Control		
User Rights Restriction	Organ.	A.11.1.1
Enhanced Password Policy	Organ.	A.11.1.1

Table 6.5.: Exemplary Risk Compositions and Mitigating Control Groups

Risk Name	**Asset**	**Vulnerability**	**Threat**	**Control**
Burst of Fire	Application Server	No Fire Suppression Control	Fire	FSC
Malware Infection	Workstation	No Virus Scanner / Updates	Malware Upload	AVC, RUC
Sabotage by Int. Threat Agent	Database Server	Lack of Phys. Protection Mechanisms	Hardware Sabotage	PPC
Data Loss due to Power Failure	Request Data	No proper Backup Strategy	Power Failure	BSC
Data Entry Error	COTS DMS	Carelessness	Error Overlooking	ETC
Network Eavesdropping	Network Infrastructure	No Network Protection	Eavesdropping	FWC
Internal Data Manipulation	Insurance Status Data	No proper Access Policy	Unauth. Data Manipulation	ACC
Offline Industrial Espionage	Request Database	Lack of Security Awareness	Social Engineering	ETC
Unwanted Money Transfer	External Web Service	Lack of Encryption Techniques	Impersonation	ECC
Unwanted Tampering with Software	Scanning Software	Malware Upload	Lack of Security Awareness	ETC

i.e. their confidentiality, integrity, and availability. A breach in either of these may result in a major image value loss. The security status is measured in points (1-1000) and is pre-calculated with the following formula:

$$Security\ Status\ Points = C_i \times I_i \times A_i, \tag{6.1}$$

where C_i represents the confidentiality, I_i the integrity, and A_i the availability requirement of asset i measured in points (1-10); the higher the requirement, the higher the value.

Process Benefit (process) This category determines the safeguards' effectiveness in keeping the assets available to be used in the business processes, i.e. the positive effect of safeguards on the process which is measured in points of process generated value.

User Acceptance (simple) The final benefit category represents a property often neglected, but nevertheless important, which can have a considerable impact on the success of safeguards: the user acceptance, measured in percent; the higher the user acceptance, the higher the value.

Apart from the beneficiary properties, the safeguards' cost efficiency has to be evaluated as well (especially important for the management) by defining the following resource categories:

Setup Costs (simple) Setup costs simply refer to the initial monetary costs of the safeguards' acquisition and implementation.

Running Costs (simple) The other type of resources measured in monetary terms is the running cost of each safeguard for each period. This can be e.g. license costs for the utilization of a specific software per year or expenses of hiring an external security expert for training sessions.

Maintenance Time Expenditure (simple) Apart from the monetary spendings, the time expenditure of safeguard maintenance, or procedure execution time (for operational safeguards) are considered. This includes e.g. the length of training sessions or the duration of backup procedures measured in hours.

Productivity Loss (process) And finally, to measure the negative impact of safeguards on the business process, the productivity loss category is specified (in points). In order to use the process-type category as a cost category, the following changes to the denominations have to be made (cf. formula 4.2): Process contribution is changed into productivity loss, process impact now measures the effect of the assets on the overall productivity of the process, and the process-related effectiveness factor describes how much the safeguards lower the assets' productivity (i.e. handicaps them).

Safeguard values for all categories are aggregated with the total-type, except for User Acceptance, which is calculated as average. All categories are marked to be optimized, i.e. safeguards are to be optimized in all categories.

After specifying the evaluation categories, the stakeholders discuss and provide the necessary quantitative data for each entity, including the following [2]:

Assets Monetary asset values (for the asset value preservation category) of tangible assets are determined by their replacement costs; intangible assets are valued according to their business impact, taken from the results of a business impact analysis. Asset values for the security status category are determined by the security requirements of each asset (table 6.6).

[2] A complete list of all quantitative data can be found in Appendix A.2.

Table 6.6.: Exemplary Asset Values

Asset	**Asset Value Preservation Category**	**Security Status Category**			
		Conf.	Int.	Avail.	total
Database Server	15000	4	8	6	192
Workstation	5000	2	6	4	48
COTS DMS	8500	2	6	6	72
Request Database	25000	8	8	6	384
Money Order Data	10000	10	10	6	600

Process impact (0-100) for both process-related categories, process benefit and productivity loss, is determined by analyzing the importance of assets for the business process (table 6.7); process value is set to 1000 points for both categories.

Table 6.7.: Exemplary Asset Impact Values

Asset	**Impact on Process Benefit**	**Impact on Productivity**
Database Server	100	100
Workstation	50	50
COTS DMS	90	90
Request Database	100	100
Money Order Data	100	100

Vulnerabilities Vulnerability exposure values (0-100) are estimated with the help of business impact analysis results (table 6.8).

Table 6.8.: Exemplary Vulnerability Exposure Values

Vulnerability	**AV Preservation**	**Sec. Status**
No Proper Backup Strategy	100	100
Lack of Security Awareness / IT Training	5	45
Lack of Encryption Techniques	80	80
No Virus Scanner / Regular Updates	15	90
No Fire Suppression Control	90	70

Threats The annual rate of occurrence of threats is estimated by security experts. Reports and statistics on security breach incidences of other organizations are used as an aid for this task. Threat AROs range from 0.1 to 200 in this case study (table 6.9).

Safeguards The safeguards setup (initial) and running costs measured in monetary terms are relatively easy to find out using vendor tenders and price lists for acquisition costs and calculations of the accounting department of the company.

Table 6.9.: Exemplary Threat AROs

Threat	ARO
Data Entry Error	200
Fire	0.1
Malware Upload	150
Eavesdropping	20
Hardware Sabotage	0.5

Maintenance times in hours are estimated by the IT experts, and user acceptance values (0-100) are determined by the system users (table 6.10).

Table 6.10.: Exemplary Simple Safeguard Values

Safeguard	User Acc.	Setup C.	Running C.	Maint. Hours
Backup A (basic)	90	5000	500	120
AV Scanner A (basic)	95	0	0	10
Firewall B	80	600	150	10
Fire Extinguisher B (fixed)	85	20000	2500	95
Security Guards	25	10000	7500	250

Furthermore, the safeguards' risk- and process-related effectiveness values (handicap percentage for productivity loss category) are determined (tables 6.11 and 6.12).

Table 6.11.: Exemplary Risk-related Safeguard Effectiveness and mitigated Risks

Safeguard	Mitig. Risk	Effectiveness	
		AV Preservation	Sec. Status
Backup A (basic)	Data Loss (Power Failure)	70	70
AV Scanner A (basic)	Malware Infection	35	75
Firewall B	Intrusion Into System	15	65
Fire Extinguisher B (fixed)	Burst of Fire	95	35
Security Guards	Sabotage	95	35

The relatively low percentage for the effectiveness of the fire extinguisher B (table 6.11) in mitigating the risk fire in the security status category can be explained as follows: As fire actually threatens mainly the availability of the asset, the effectiveness can only reach about one third of 100. Therefore the fire extinguisher is assigned a value of 35, meaning that this control protects the asset from fire almost perfectly.

As the final task of phase 2, any necessary constraints and interdependencies are specified:

Table 6.12.: Exemplary Process-related Safeguard Effectiveness and affected Assets

Safeguard	**Affected Asset**	**Effectiveness**	
		Proc. Benefit	Prod. Loss
Backup A (basic)	Request Data	85	0
AV Scanner A (basic)	Request Data	55	35
Firewall B	Network Infrastr.	75	20
Fire Extinguisher B (fixed)	Workstation	95	0
Security Guards	Workstation	95	10

Category Limits Upper limits for the aggregated costs of the safeguard portfolios are set by the management to 40000 (setup costs) and 15000 units (running costs). The maximum aggregated maintenance time is restricted to 1500 hours.

Constraints concerning the portfolio composition Just exactly one member of the following control groups is allowed and required in the solution because of mutual exclusiveness: BSC Backup Strategy, RUC Regular Virus Signature Updates, ECC Encryption, FWC Firewall Protection, SLC Server Event Logging, and FSC Fire Suppression. At least one item of the following groups is required (more are allowed): AVC Virus Scanner, PPC Physical Protection, ARC Access Rights Policy, and MFC Maintenance and Fallback Equipment. Only Fallback Equipment Set A or B (MFC) may be included, but not both. The same applies to the ETC Employee Training methods.

Interdependencies The following synergy effects may be triggered: If both AVC AV Scanner B and FWC Firewall B are acquired, Vendor B grants a total price discount of about 10%. Combining both elements of ARC, User Rights Restriction and Enhanced Password Policy, results in an improvement of their security status values by 50%. Finally, adding a second or even third virus scanner would not yield a doubling or tripling of their performance, but merely in a minor improvement, realized by an adequate reduction of the overall asset preservation and security status values of the portfolio if more than one virus scanner is selected.

This concludes the risk assessment process and the second phase of the MR-MOD framework.

6.4. Phase 3

When all entities and quantitative data as well as all constraints and interdependencies are entered into the MODStool software, the search for non-dominated solutions can begin and phase 3 of the MR-MOD framework begins. All major decision makers including members of the management and IT/security experts are present. The other participants of the workshop process are dismissed, as the data gathering phase is completed.

With 30 individual safeguard candidates specified, there are $2^{30} = 1073741824$ different possible combination, whose evaluation would take a considerable amount of time. Because of the mechanics of MODStool, any non-valid solutions, i.e. those that violate any inclusion and/or exclusion constraints and category limits, are ignored before they are tested for Pareto-dominance, thus reducing the overall duration of the calculation significantly.

The optimization process yields 9769 non-dominated solutions. To further reduce the number of portfolios, the following limits are imposed on the solutions:

- The upper limit for total setup costs is lowered from 40000 to 30000 units.
- The upper limit for total running costs is lowered from 15000 to 9000 units.
- The upper limit for total maintenance time expenditure is set to 800 hours.
- An upper limit for total productivity loss is set to 2500 points.
- A lower limit for average user acceptance is set to 75 percent.

Complying with these constraints, 302 solutions remain (figure 6.3). The green bars in the upper boxes represent the aggregated values of the remaining portfolios in the benefit categories, the orange bars in the lower boxes the values in the cost categories. The larger red horizontal bars with arrows define the upper and lower limits for each category. The smaller brown horizontal bars left to the green/orange vertical bars indicate the category values of each of the 9769 non-dominated solutions. The small red horizontal bars below the brown bars represent the category values of the initial safeguard portfolio already in use, indicating that this portfolio produces lower values in all categories, except for user acceptance, where the value is greater.

To obtain the best solutions regarding asset value preservation and security status, the lower limits are increased until only 6 portfolios remain, shown in table 6.13 and figure 6.4. Analyzing the solutions, there are only minor differences between them: All of them include Backup A (basic), Daily Virus Signature Updates, both Virus Scanners B and C, SK Encryption, Portable Fire Extinguishers, Physical Locks, and Enhanced Password Policy. None includes Employee Training, neither basic nor extensive, as their

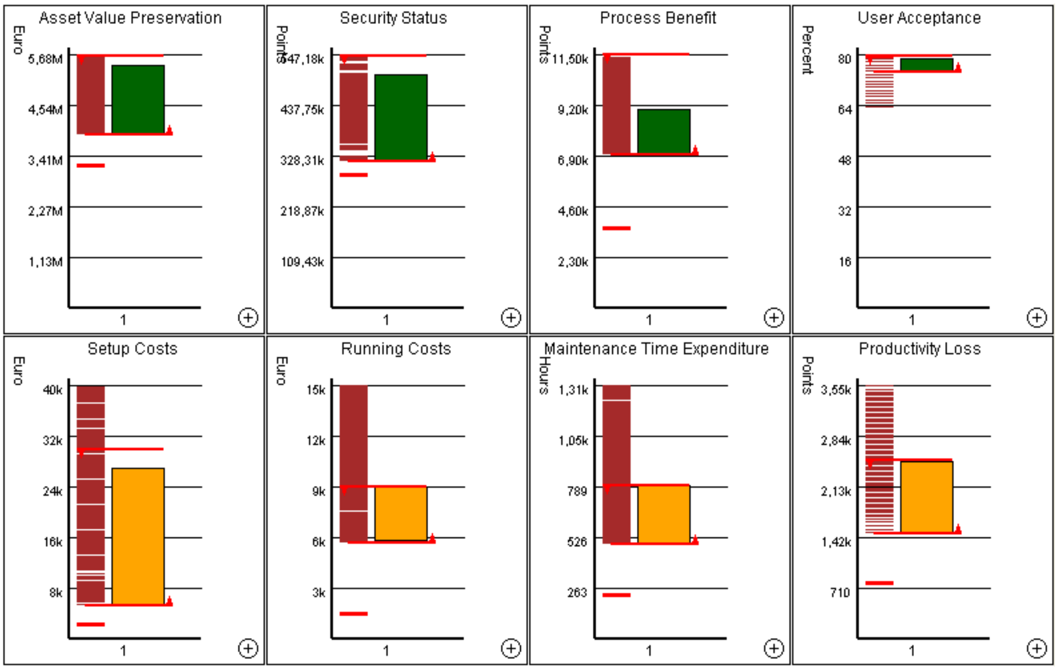


Figure 6.3.: Pareto-optimal Portfolios after imposing Category Limits

influence on the benefits is relatively low compared to their costs. On the contrary, using both Virus Scanners B and C seems beneficial because of their boost to the benefits with relatively low resource demands. Safeguards of high resource requirements such as Fixed Fire Suppression Control and Full Fallback Equipment Set are too expensive for the benefits they provide.

Comparing the benefit category values of the portfolios, there are only minor deviations within a few percent. As for the setup costs and maintenance time expenditures, the situation is different: Setup costs of Portfolio 1 and 3 are almost twice as high as those of the others due to the Basic Fallback Equipment, and Portfolio 1, 2, and 5 require about 10 to 20 percent more maintenance hours than the other two. With these numbers in mind, Portfolio 4 and 6 are the optimal solutions for this case study with respect to all given categories, especially when comparing them with the best performing solutions of the 9769 non-dominated portfolios with roughly the same values in asset value preservation (about 5500000 units) and under 10 percent less security status points (about 540000), but with more than four times the setup costs (about 38000 units) and roughly twice the running costs (just under 15000 units), as well as about 30 percent higher maintenance time demands.

In comparison with the initial portfolio, the new portfolios almost double the asset value preservation and security status, and nearly triple the process benefit, but at the

Table 6.13.: Composition of the Top 6 Portfolios and Values

Control / Category	**PF 1**	**PF 2**	**PF 3**	**PF 4**	**PF 5**	**PF 6**
BSC	Backup A	Backup A	Backup A	Backup A	Backup A	Backup A
MFC	Basic Fallback	Regular Maint.	Basic Fallback	Regular Maint.	Regular Maint.	Regular Maint.
RUC	Daily	Daily	Daily	Daily	Daily	Daily
AVC	B+C	B+C	B+C	B+C	B+C	B+C
ECC	SK	SK	SK	SK	SK	SK
FWC	Firewall D	Firewall D	Firewall D	Firewall D	Firewall B	Firewall B
SLC	Full	Full	Fault	Fault	Full	Fault
FSC	Port.	Port.	Port.	Port.	Port.	Port.
PPC	Physical Locks	Physical. Locks	Physical Locks	Physical Locks	Physical Locks	Physical Locks
ETC	x	x	x	x	x	x
ATC	PW Pol.	PW Pol.	PW Pol.	PW Pol.	PW Pol.	PW Pol.
Asset Value	5431167	5455776	5405776	5430376	5444526	5419126
Sec. Status	506584	506610	505468	505494	505150	504034
Proc. Benef.	8355	8505	8205	8355	8605	8455
User Acc.	76	75	77	76	75	75
Setup C.	13050	8050	13050	8050	7550	7550
Runn. C.	8370	8270	8270	8170	8270	8170
Maint.	715	695	615	595	675	575
Prod. Loss	2250	2250	2200	2200	2350	2300

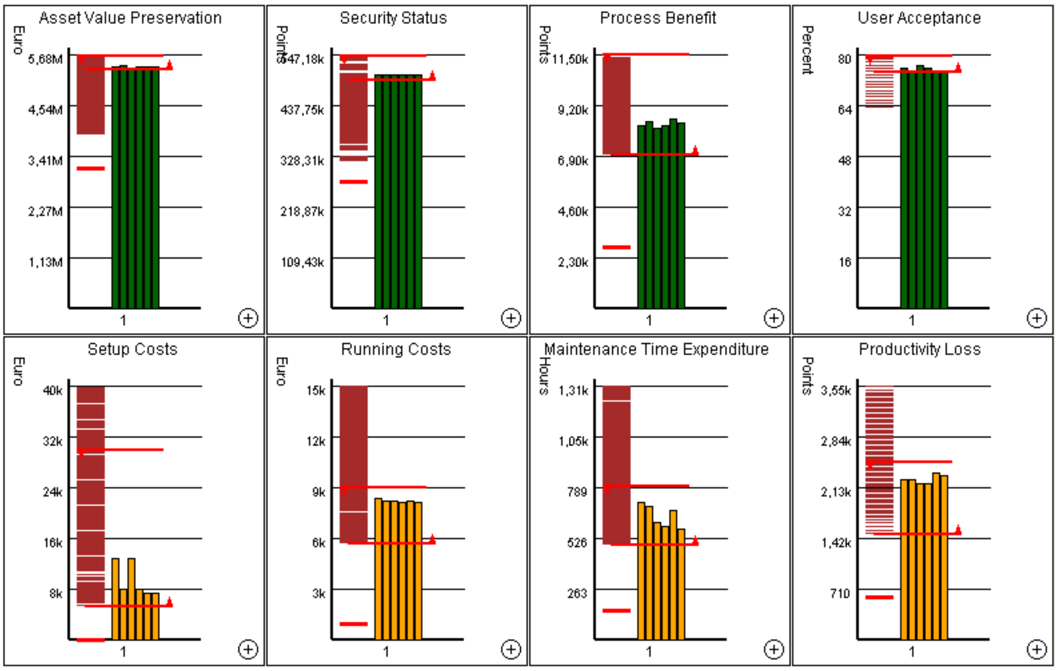


Figure 6.4.: Top 6 Portfolios regarding Asset Value Preservation and Security Status

expense of existing setup costs (0 for the initial portfolio), almost nine times higher running costs, and more than threefold the maintenance time and productivity loss. User acceptance is also a bit worse.

6.5. Remarks

The results of the calculation may react quite sensitive to certain data changes under certain circumstances: Reviewing the threat AROs of this case study (table 6.9), Malware Infection (150), Data Entry Error (200), and Error Overlooking (100) are estimated to occur quite often. To demonstrate the data sensitivity of the calculation, the ARO of the threat Malware Infection is reduced to 50, and in the next step Data Entry Error set to 50 and Error Overlooking to 20. Figure 6.5 reveals the differences in the category values of the non-dominated solutions, where the top row shows the benefit categories with unmodified AROs, the middle row the results with reduced Malware Infection, and the bottom row the results when additionally lowering the AROs of Data Entry Error and Error Overlooking.

As the ARO only affects risk-related categories, no changes in process benefit and user acceptance can be observed. But the solution values of asset value preservation and security status are roughly halved, only by modifying a single ARO. This is due to the relatively high exposure factors of vulnerabilities related to Malware Infection and the relatively high frequency of this threat in risks.

Comparing the middle and lower rows, no major differences are to be found, although two AROs are considerably reduced additionally. The reason for this behavior is the low impact of the vulnerability Carelessness associated with these threats, with exposure factors of only 5 and 15 percent, thus having a smaller influence on the overall category values.

Considering these results, input data has to be estimated very accurately, especially the probabilities of threats (i.e. AROs) which are often hard to judge due to the lack of suitable statistics and data. Depending on the composition of the risks, the assets' values, and the vulnerabilities' exposure factors, entering a single inaccurate data entry may result in dramatically different solutions.

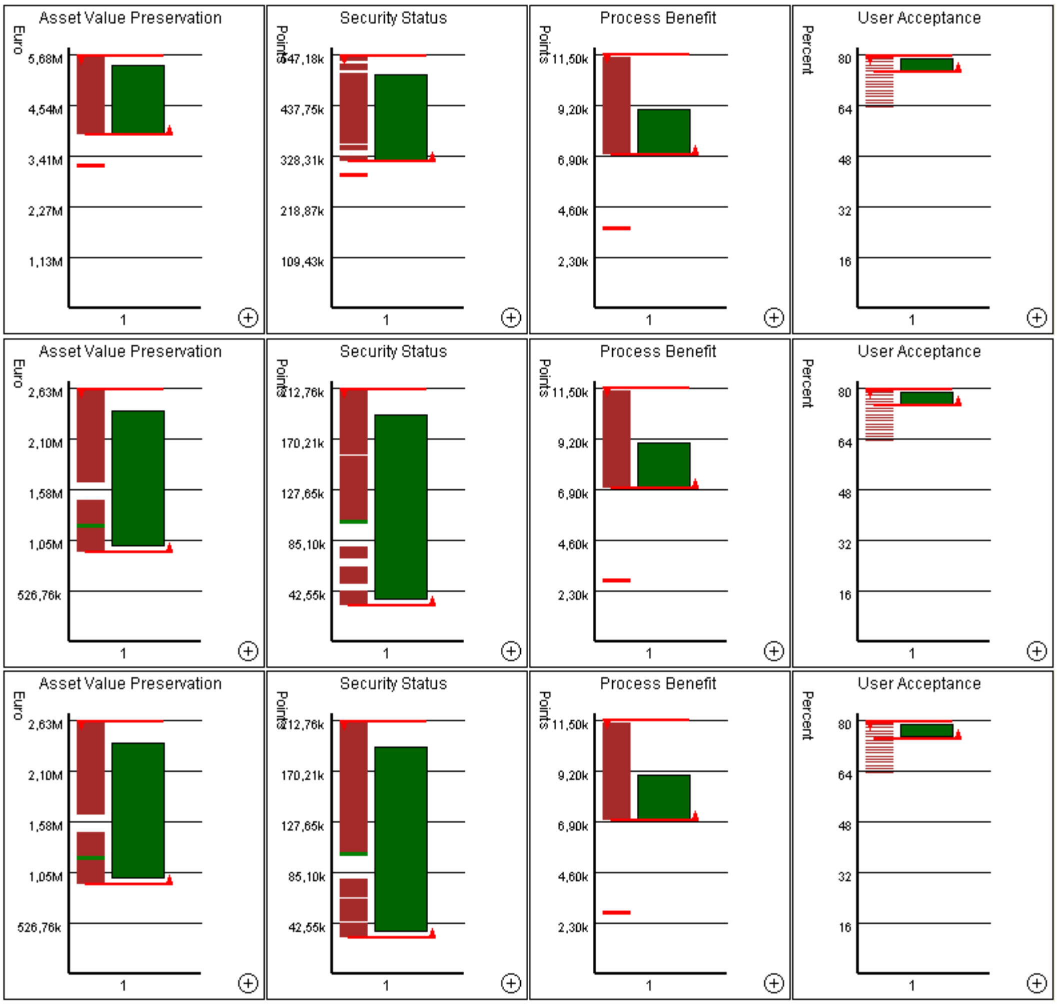


Figure 6.5.: Effects of lower and higher AROs of Malware Infection, Data Entry Error, and Error Overlooking

7. Comparison of the Proposed Method with other Frameworks

In this chapter, MR-MOD is compared with two other methodologies, namely the decision support process AHP (section 3.1) and the security evaluation and requirements elicitation framework POSeM (section 3.2). In the following, they are applied to the same test scenario of the previous chapter (with certain adjustments) and their methods of operation analyzed. Finally, the differences of all three frameworks regarding functions and results are described.

7.1. AHP

The AHP is selected for comparison because of its popularity and widespread use as a tool for solving decision making problems. The cost and benefit categories of the MR-MOD case study are used as high-level criteria and some are further divided into sub-criteria. As the number of alternatives (safeguard list of the MR-MOD case study) exceeds the proposed maximum limit of nine items for direct comparison, the ratings mode of AHP is used for evaluating the alternatives (the criteria's weights are determined by direct pairwise comparison as usual). For each low-level criterion, different 5 step rating scales are developed to convert the quantitative values of the MR-MOD case study into qualitative intensities. The alternatives are assigned their ratings by comparing their quantitative values for each criterion with the criterion's step function.

7.1.1. Step 1: Hierarchies

In this case, two separate hierarchies for benefit and cost criteria are defined.

Benefit Hierarchy

The main goal node of the benefit hierarchy is: Evaluate alternatives to improve business process security according to their benefits. The criteria and sub-criteria are defined as follows:

1. **Asset Value Preservation** This criterion defines how well the alternatives protect asset values, and it is divided into the following sub-criteria:
   - Asset Value (very low to very high) is determined by the aggregated values of those assets the alternatives are assigned to.
   - Risk Reduction (very low to very high) refers to the alternatives' sum of all risk reduction values of all mitigated risks[1].
   - Number of protected Assets (single to many) defines the total number of assets that are protected by each alternative.
2. **Security Status** This criterion defines the alternatives' contribution to the overall security status (very low to very high):
3. **Process Benefit** This criterion defines the alternatives' benefit to the business process and is divided into the following sub-criteria:
   - Asset Importance (low to absolute importance) is determined by the impact of assets protected by the alternatives (geometric mean if an alternative protects multiple assets).
   - Protection Effectiveness (very low to very high) refers to the effectiveness of alternatives to preserve the asset's availability for the business process (geometric mean if an alternative protects multiple assets).
4. **User Acceptance** This criterion defines how well the alternatives are accepted (virtually unaccepted to completely accepted).

Cost Hierarchy

The main goal node of the cost hierarchy is: Evaluate alternatives to improve business process security according to their resource demands. The criteria and sub-criteria are defined as follows:

[1] (Asset Value * Vulnerability Exposure * Threat ARO) * Safeguard Effectiveness

1. **Setup Costs** This criterion defines the amount of the alternatives' setup costs (none to very high).
2. **Running Costs** This criterion defines the amount of the alternatives' running costs per period (none to very high).
3. **Maintenance Time** This criterion defines the maintenance time demands of alternatives per period (very low to very high expenditure).
4. **Productivity Loss** This criterion defines the productivity loss resulting from implementing the alternatives, and it is divided into the following sub-criteria:
    - Asset Impact (low to full impact) is determined by the impact of an asset's unavailability on the productivity of the business process (geometric mean if an alternative impedes multiple assets).
    - Safeguard Impediment (no to major impediment) refers to the extend of alternatives to impede the fulfillment of the asset's tasks (geometric mean if an alternative impedes multiple assets).

7.1.2. Step 2: Criteria Prioritization

In the next step, all sub(criteria) of both hierarchies are assigned priorities according to their importance by pairwise comparison (e.g. table 7.1[2]).

Table 7.1.: Asset Value Preservation Criterion

Asset Value Preservation	**Asset Value**	**Risk Reduction**	**Nr. of Assets**	**Priority**
Asset Value	1	3	2	0,249
Risk Reduction	1/3	1	3	0,594
Nr. of Assets	1/2	1/3	1	0,157

Both hierarchies with all elements and their local priorities are shown in figure 7.1.

7.1.3. Step 3: Alternative Evaluation

For dealing with the 30 alternatives, applying the pairwise comparison technique is unfeasible. Therefore, the ranking method of AHP is applied using step functions to assign each alternative an appropriate intensity level for each criterion according to their quantitative values used in the MR-MOD case study. The following intensity levels and step limits are defined for the benefit criteria:

[2] All comparisons are listed in Appendix A.3.

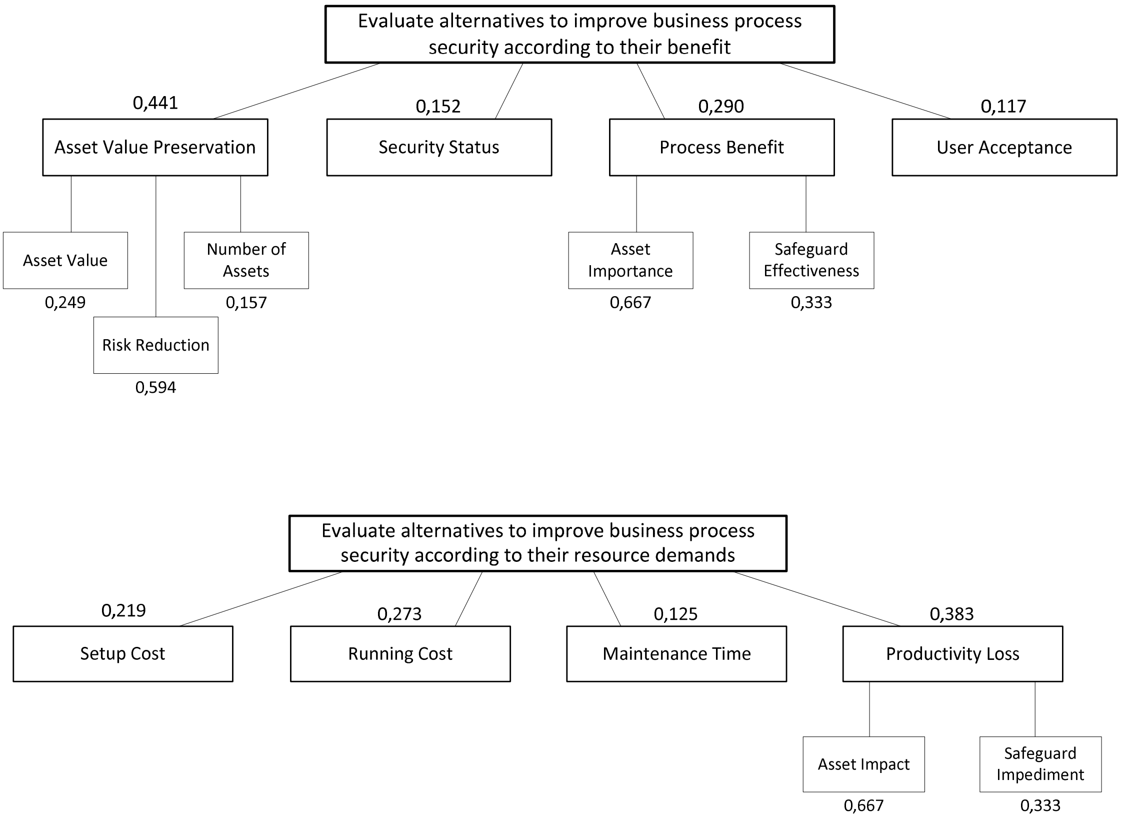


Figure 7.1.: Benefit and Cost Hierarchies

Asset Value (AV Pr.) very low (0-24999), low (25000-49999), medium (50000-74999), high (75000-99999), very high (100000 and above)

Risk Reduction (AV Pr.) very low (0-49999), low (50000-99999), medium (100000-199999), high (200000-499999), very high (500000 and above)

Number of Protected Assets (AV Pr.) single (0-1), few (2-3), some (4-6), several (7-9), many (10 and above)

Security Status very low (0-9999), low (10000-19999), medium (20000-49999), high (50000-99999), very high (100000 and above)

Asset Importance (Proc. Benefit) low importance (0-49), some importance (50-69), significant importance (70-89), major importance (90-99), absolute importance (100)

Protection Effect. (Proc. Benefit) very low (0-49), low (50-69), medium (70-89), high (90-99), very high (100)

User Acceptance virtually unaccepted (0-49), reasonably well accepted (50-69), well accepted (70-89), very well accepted (90-99), completely accepted (100)

For the cost criteria, the following intensity levels are specified:

Setup Costs none (0), low (1-4999), medium (5000-9999), high (10000-19999), very high (20000 and above)

Running Costs none (0), low (1-999), medium (1000-4999), high (5000-9999), very high (10000 and above)

Maintenance Time very low (0-49), low (50-99), medium (100-199), high (200-299), very high (300 and above)

Asset Impact (Prod. Loss) low impact (0-49), some impact (50-69), significant impact (70-89), major impact (90-99), full impact (100)

Safeguard Imp. (Prod. Loss) no impediment (0), low impediment (1-4), medium impediment (5-9), high impediment (10-19), very high impediment (20 and above)

Some values are shown in table 7.2[3].

[3] A full listing can be found in the Appendix A.3.

Table 7.2.: Some Alternative Priorities (Benefit Criteria)

Alternative	Risk Red.	Sec. Status	Asset Imp.	User Acc.
Backup A	0,343	0,112	1,000	0,627
Regular Maint.	0,199	0,112	0,627	0,382
SK Encrypt.	0,199	0,195	0,232	0,382
Firewall D	0,343	0,627	0,627	0,627
Fault Logging	0,589	0,335	0,232	0,382

7.1.4. Step 4: Global Priorities

With the local priorities for all alternatives and criteria, the global priorities can be synthesized, using the ideal mode. The top 10 performing alternatives are displayed in figure 7.2: The upper part shows the best 10 alternatives regarding their benefits and the lower part the highest rated regarding their resource demands.

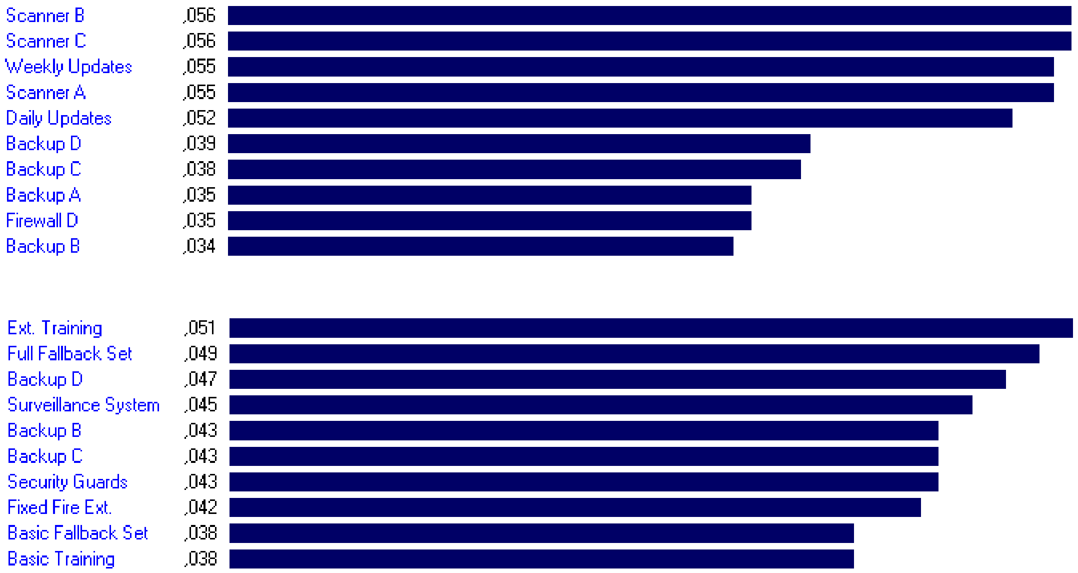


Figure 7.2.: Highest Rated Alternatives (Global Priorities)

Dividing the global benefit priorities by the global cost priorities, the overall priorities can be determined and are listed in table 7.3. Comparing these numbers with the MR-MOD case study and applying similar constraints, i.e. to select the best performing alternative of each group for the final portfolio, AHP produces similar results: Backup A, SK Encryption, Full Logging, Portable Fire Extinguisher, Physical Locks, and Enhanced Password Policy safeguards are included in all top 6 solutions of the MR-MOD case study; Regular Maintenance and Firewall D are selected for some. Only in group RUC and AVC, there are differences to be found: In contrast to MR-MOD, AHP prefers

Weekly Updates and Virus Scanner A.

Table 7.3.: Overall Ranking of Alternatives

Alternative	Group	Benefit Rating	Cost Rating	Overall
Backup A	BSC	0,035	0,033	1,061
Backup B	BSC	0,034	0,043	0,791
Backup C	BSC	0,038	0,043	0,884
Backup D	BSC	0,039	0,047	0,830
Reg. Maintenance	MFC	0,028	0,034	0,824
Basic Fallback Set	MFC	0,027	0,038	0,711
Full Fallback Set	MFC	0,029	0,049	0,592
Weekly Updates	RUC	0,055	0,021	2,620
Daily Updates	RUC	0,052	0,027	1,956
Scanner A	AVC	0,055	0,024	2,292
Scanner B	AVC	0,056	0,029	1,931
Scanner C	AVC	0,056	0,029	1,931
SK Encryption	ECC	0,021	0,026	0,808
PK Encryption	ECC	0,022	0,030	0,733
Firewall A	FWC	0,030	0,026	1,154
Firewall B	FWC	0,033	0,030	1,100
Firewall C	FWC	0,033	0,030	1,100
Firewall D	FWC	0,035	0,030	1,167
Firewall E	FWC	0,031	0,034	0,912
Fault Logging	SLC	0,027	0,020	1,350
Full Logging	SLC	0,033	0,022	1,500
Port. Fire Ext.	FSC	0,027	0,025	1,080
Fixed Fire Ext.	FSC	0,028	0,042	0,667
Physical Locks	PPC	0,026	0,027	0,963
Surveillance Sys.	PPC	0,025	0,045	0,556
Security Guards	PPC	0,025	0,043	0,581
Basic Training	ETC	0,023	0,038	0,605
Ext. Training	ETC	0,026	0,051	0,510
User Rights Restr.	ACC	0,025	0,038	0,658
Enh. Password Pol.	ACC	0,025	0,029	0,862

7.2. POSeM

POSeM's focus on business process components as requirements elicitation basis for security renders it interesting to be compared to the functionality of process models in the MR-MOD framework. For POSeM, the process model and its components (actors, activities, data assets) of the MR-MOD case study are used as input for the security evaluation, and the safeguard list is extended to 50 items to better suit the focus on the 'requirements' elicitation process of this framework. The other elements of the MR-MOD test scenario, cost and benefit categories, risk information, and quantitative data, cannot be implemented and are ignored.

7.2.1. Step 1: General Security Objectives

The first step of POSeM consists of the definition of general security requirements regarding confidentiality, integrity, availability, and accountability of process components:

Confidentiality The business process of interest mainly deals with sensitive customer data (name, address, financial data,...), and therefore, actors and activities handling this information need to have relatively high confidentiality requirements, as well as the data itself. Components related to money orders should be regarded as very high confidential.

Integrity Apart from confidentiality, integrity is of prime importance for customer data accounting processes in the financial sector and crucial for the success of the business. Thus, integrity levels should be high, and again very high for money-related artifacts and processing activities and actors.

Availability Although high availability and therefore lower process cycle times are surely beneficial, for this test scenario it is not of utmost importance, because disruptions are considered as minor problems (if within reasonable times). Therefore, basically low to medium availability levels for the process components are considered sufficient.

Accountability Similarly to availability, accountability is basically not one of the greatest concerns for this business process (except for certain components) and medium levels are sufficient.

7.2.2. Step 2: SEPL Model

As required by the POSeM framework, all relevant components of the business process are identified and described with the SEPL, and they are assigned clearance and security levels for each of the security attributes. The initial levels for each entity are listed in table 7.4, 7.5, and 7.6.

7.2.3. Step 3: Consistency Check

For the next step, the consistency check, only the simple level rules of the 'greater or equal' type are used in the RB1, defining that activities must have security requirement

Table 7.4.: Initial Clearance Levels for Actors (Participants)

ID	Participant	Type (opt.)	Conf.	Int.	Avail.	Acc.
p1	Preparer	Human	high	med	med	med
p2	Assistant	Human	med	med	med	med
p3	Supervisor	Human	very high	very high	med	high
p4	E-Mail System	System	med	med	low	high
p5	Ext. Web Service	System	very high	very high	med	high

Table 7.5.: Initial Security Levels for Activities

ID	Activity	Type (opt.)	Conf.	Int.	Avail.	Acc.
a1	Register Request		high	med	high	med
a2	Check Request for Eligibility		high	high	med	med
a3	Return Request to Applicant	Transfer	med	med	med	med
a4	Scan Request		med	high	med	med
a5	Check Request for Uniqueness	Storage	high	high	med	med
a6	Process Request		med	med	med	med
a7	Mark for Approval		med	med	med	med
a8	Open Marked Documents (SV)		high	high	med	high
a9	Edit Request		med	med	med	med
a10	Check Correctness		high	high	med	med
a11	Inform Applicant	Transfer	med	med	med	med
a12	Send Money Order	Transfer	very high	very high	med	high

Table 7.6.: Initial Security Levels for Artifacts (Data)

ID	Data	Type (opt.)	Conf.	Int.	Avail.	Acc.
o1	Request Data	Data	high	high	med	med
o2	Request Data (DB)	Data	high	high	med	med
o3	Applicant's Insurance Status	Data	high	high	med	med
o4	Money Order Data	Data	very high	very high	med	high
o5	Request Return Mail	Data	med	high	low	med

levels greater or equal than that of the processed data, and participants clearance levels greater or equal than that of the assigned activities, e.g. (in SCRL):

```
RULE r1
  PARCICIPANT CONFIDENTIALITY
    GEQ ACTIVITY CONFIDENTIALITY
END_RULE
```

The checking process revealed several inconsistencies in the triplets, mostly because of confidentiality and integrity clearance/security levels of participants and activities being to low for matching the levels of the Request Data (e.g. table 7.7).

Table 7.7.: Consistency Check of the triplet Preparer/Register Request/Request Data

ID	Component	Type (opt.)	Conf.	Int.	Avail.	Acc.
p1	Preparer	Human	high	med	med	med
a1	Register Request		high	med	high	med
o1	Request Data	Data	high	high	med	med
			ok	error	error	ok

Basically, there are two alternatives to solve the inconsistencies, either to raise the requirement levels of participants and activities, or to lower those of the Request Data. In accordance with the general security objectives defined in step 1, the security levels are increased[4].

7.2.4. Step 4: Safeguard Derivation

Within the RB2 for deriving suitable security measures, all 50 safeguards are categorized into 10 different modules defining their application (cf. [Röh03]), and modules to be applied to the process components are selected. Some of the controls and their security levels are listed in table 7.8[5].

Applying RB2 on the process components, a total of 36 suitable security measures are derived. As the security requirements for this business process are relatively high (for confidentiality and integrity), almost all safeguards are applicable; the main reason for the reduction from 50 to 36 are 'obsoletes'-statements. The other safeguards not selected are only needed in an ultra high security environment, such as Backup Power Generators in a hospital where a possible power failure directly threatens human lives.

[4] A full listing of the consistency check tables and all level changes can be found in the Appendix A.4.

[5] A full listing of the module assignment and available controls can be found in the Appendix A.4.

Table 7.8.: Selected Security Safeguard Derivation Rules (RB2)

		Conf.			**Int.**			**Avail.**			**Acc.**		
ID	**Control**	**P**	**O**	**A**	**P**	**O**	**A**	**P**	**O**	**A**	**P**	**O**	**A**
t1a	Basic Empl. Training	2H	-	-	2H	-	-	2H	-	-	2H	-	-
t1b	Ext. Empl. Training	3H	-	-	3H	-	-	3H	-	-	3H	-	-
e1a	Port. Fire Extinguisher	-	-	-	-	2	-	-	2	-	-	-	-
e1b	Fixed Fire Extinguisher	-	-	-	-	3	-	-	3	-	-	-	-
e4	Physical Locks	2S	2	2	2S	2	2	2S	2	2	2S	2	2
o3a	Backups (basic)	-	-	-	-	-	-	1S	1	1S	-	-	-
o3c	Backups (double)	-	-	-	-	-	-	4S	4	4S	-	-	-
v1a	Virus Scanner A	1	1	1	1	1	1	1	1	1	1	1	1
v1b	Virus Scanner B	2	2	2	2	2	2	2	2	2	2	2	2
v1c	Virus Scanner C	2	2	2	2	2	2	2	2	2	2	2	2
n2	Penetration Testing	4	4	4T	4	4	4T	4	4	4T	4	4	4T
c1	SK Encryption	3	3D	3	3	3D	3	-	-	-	3	3D	3
c2	PK Encryption	4	4D	4	4	4D	4	-	-	-	4	4D	4

7.3. Findings

The following section analyzes the three methodologies MR-MOD, AHP, and POSeM, and their results of the test scenario evaluation in terms of the following aspects:

Mechanics of Safeguard Evaluation Although all three methodologies can be applied to derive suitable safeguards, their modes of operation are completely different: POSeM applies a rule-based derivation depending on security requirements and clearance levels of process components to determine suitable safeguards. POSeM also provides functions to check the individual components on security requirement consistency using another rule-base generally defining 'greater or equal'-relations. But it can also include complex composed rules.

AHP is a decision support method for dealing with multiple objectives, and it relies on the pairwise comparison of each safeguard, called alternatives, with respect to the multiple objectives, called criteria. These criteria can be divided into several sub-criteria building a hierarchy to increase the complexity and expressiveness of the decision model. By pairwise comparing the criteria of the same level, a ranking of importance can be established, which is applied on the safeguards to determine the global priorities of each safeguard with respect to all criteria.

MR-MOD also applies decision making techniques, but it is based on the concept of Pareto-dominance to deal with the multiobjective nature of the safeguard evaluation. It is developed as a quantitative method that includes a risk assessment phase to determine risk-related data such as asset values and threat AROs to be used as a decision criterion for the safeguard candidates. Apart from these risk-related issues, other properties of safeguards can be defined as optimization objectives as well, including their influence on business processes. In contrast to POSeM (providing a list of suitable safeguards) and AHP (providing a ranking of safeguards with respect to criteria), MR-MOD produces a set of the most effective safeguard combinations possible.

Completeness As these three frameworks derive safeguards differently, they also focus on different aspects of security evaluation: POSeM focuses on business process models, expressed as lists of actors, artifacts, and activities, and their requirements in security attribute categories, i.e. confidentiality, integrity, availability, and accountability. In contrast to risk-based methodologies, any specific threats to process components are completely neglected, as well as physical assets worth being protected, such as the IT infrastructure required for the business process. Furthermore, other properties of safeguards such as their cost effectiveness are not considered either.

AHP was not specifically developed to deal with information security and safeguard evaluation, but can be used for virtually any decision problem. Like all tools that can be used universally, AHP lacks security specific functions, and there is no inherent consideration of business processes in the standard AHP framework. This can be compensated by defining suitable criteria and sub-criteria that represent any security- and process-related issues, which have to be specified in such a way that the alternatives can be directly compared to each other (or ranked) with respect to each criterion.

In contrast to AHP, MR-MOD is specifically designed to evaluate candidates in a process-related and security-specific environment. Therefore, it provides means for evaluating all risk-related entities (assets, vulnerabilities, threats), as well as process-related issues (influence of safeguards on processes). Like POSeM, MR-MOD relies on process models as the basis for the evaluation, but unlike POSeM, it does not consider actors, but specific threats and vulnerabilities. Furthermore, POSeM's artifacts can be modeled as data-type assets, and MR-MOD also takes physical assets into consideration.

Security Insight A desirable side effect of security-related evaluation procedures is the participants' gain of insight into security matters, which can be provided by POSeM, AHP, and MR-MOD as well: By relying on the well-known and well-established CIA properties, POSeM requires participants with a good knowledge of the security requirements of the process components and/or people that are ready to deal with CIA, which provides an overall understanding of security matters. What is missing is the consideration of definite threats; no answer is given on what the process is actually protected against.

AHP may suffer from the same threat problem as POSeM due to the actual non-consideration of specific threats. This can be circumvented by defining threat specific criteria. Generally speaking, the degree of insight into security matters given by the application of AHP depends on the criteria defined by the decision makers, e.g. by defining CIA attributes as criteria, the decision makers have to be concerned with how the alternatives affect the CIA levels. Still, this can be problematic in certain cases because of the pairwise comparison technique, e.g. determining whether a fire extinguisher or a virus scanner fares better in maintaining data integrity and to what extend. The ranking method of AHP weakens this problem by replacing the pairwise comparisons of alternatives.

MR-MOD provides a profound insight into security situation of the process. It includes the definition and valuation of assets and their vulnerabilities, specific threats and their estimated rate of occurrence, and safeguard effectiveness. By composing risks, it is always clear which assets are exposed to which threats exploiting which vulnerabilities, and which safeguards are effective in mitigating these risks. MR-MOD also provides data on the influence of safeguards on business processes, both positive and negative, which is often neglected by other frameworks. Finally, economic factors such as resource requirements of safeguards are considered as well, providing a comprehensive view of the safeguards' attributes and performance levels, and of the overall security situation of the business process.

Input Data POSeM processes only qualitative data, i.e. the security requirements and clearance levels of the process components, and it does not require any quantitative data in order to complete the evaluation process.

AHP basically relies on qualitative information on the importance/probability of alternatives for the evaluation, called intensity levels. But in contrast to POSeM, AHP is able to process quantitative data as well, as demonstrated in the AHP example earlier in this section. For that case, quantitative values of alternatives are translated into intensity levels according to criterion specific step functions, using the ranking mode.

MR-MOD relies fully on quantitative data and requires complete datasets for numerous entities including asset values and vulnerability exposure factors for each risk-related category, impact of each asset on each process-generated value, and safeguard effectiveness estimates for each mitigated risk.

Consideration of Constraints and Interdependencies POSeM, AHP, and MR-MOD deal with and consider constraints and interdependencies of safeguards in different ways: POSeM only allows two kinds of dependencies regarding security measures, 'obsoletes' and 'depends on' relations, specifying which safeguards become obsolete because of others and which safeguards depend on the existence of others. Synergy or cannibalism effects of multiple safeguards are not considered.

AHP does not consider dependencies at all; it assumes that all alternatives and criteria are independent. Therefore, no constraint or interdependency can be expressed, but the successor of AHP, the Analytic Network Process (ANP) has been developed to specifically deal with these factors.

MR-MOD supports the specification of constraints and interdependencies. Constraints can be defined as the minimum or maximum number of safeguards out of a specific list that have to be or are allowed to be included in the Pareto-optimal solution. Interdependencies are defined as the minimum or maximum number of safeguards out of a specific list that are needed or allowed to trigger certain synergy or cannibalism effects on category values, e.g. a discount on the acquisition costs for certain safeguard combinations.

Individual Strengths and Weaknesses Following different concepts of defining Secure Business Processes, the three methodologies obviously have different strengths and weaknesses: POSeM excels at eliciting the security requirements of processes by analyzing all individual process components for the well-known CIA attributes, and it does not require any quantitative data, nor does it rely on extensive calculations to determine suitable safeguards. While it was specifically designed to evaluate security measures according to security requirements, it is only capable of doing exactly that, namely to propose a list of security preserving techniques / technologies that are technically suitable for the requirement levels of the process components. Whether the safeguards are cost-effective or better than any other ones is not answered, i.e. safeguards are generally not treated as alternatives the decision makers may choose from and no direct comparison is drawn between them. The POSeM example earlier in this section illustrates this lack of decision support: When comparing the three virus scanners A-C (v1a-c, table 7.8), B and C are defined as more advanced than A, being required only for CIAA levels of medium(2) instead of low(1). Thereby, a clear distinction can be observed between A and B/C. Comparing B with C is different: Assuming that their levels are equal, there is no way to make out any differences; both scanners are suitable for medium security levels and no decision can be made on which one is better by e.g. analyzing other scanner properties such as resource demands. POSeM is by no means a technique to compare safeguards with each other. Another issue with POSeM is the necessity to check whether certain safeguards are really necessary. Taking Penetration Testing (n2, table 7.8) as an example, this safeguard is required because of the activity a12 'Send Money Order' only. Therefore, it remains to be questioned, whether it is really necessary to apply Penetration Testing because of this single activity, or whether it makes more sense to drop this safeguard because 'Send Money Order' is already protected by other security measures. These considerations are subject to the optional step 5 of the POSeM framework, but no specific procedures are given. Finally, a POSeM evaluation model may reach a very high level of complexity, especially when defining complex composed rules for consistency checking, which makes the application of POSeM quite tedious without a suitable automation tool.

AHP is a well-known and widespread decision support technique that enjoys great popularity among decision makers because of its relative simplicity and adaptability to all kinds of application domains. It can be used with both qualitative and quantitative input data, and it can be combined with other techniques to provide a more powerful and domain specific decision support or evaluation tool. Unlike POSeM, it provides the decision makers with an evaluation and ranking of different comparable alternatives with respect to criteria that can be defined freely to satisfy any needs, as long as these criteria are independent of each other. The ranking not only determines which alternatives are best, but also to what extend. However, used as a standalone technique, AHP has several drawbacks when applying it on information security. Apart from the rank reversal problem, which has already been discussed in section 3.1, AHP does not include any security specific functions; it does not consider any specific threats or vulnerabilities, nor does it specifically support the evaluation of business processes and their security properties. If defined as suitable criteria, these factors are considered, but still pre-calculations have to be done (e.g. Risk Reduction values (AVP) taken from the MR-MOD case study) to get the appropriate data. If not used as criteria, these security-specific information is ignored. Another problem with AHP is the fact that all alternatives have to be directly comparable to each other when performing the pairwise comparisons on them, which is problematic if one has to compare different safeguard types as alternatives such as human security guards with the technology of packet filtering firewalls. Furthermore, AHP only ranks the individual alternatives according to their performance / importance, and it cannot suggest a complete optimal set of alternatives (portfolio), which can be of major importance for the decision makers. As the AHP example above has shown, there is a need for additional constraints, e.g. assigning the alternatives to certain groups from which the highest rated safeguards are to be selected. Otherwise, composing an optimal portfolio is a difficult task: Even though multiple properties of alternatives can be considered (including non-technical such as costs as well), AHP does not provide any aggregated values, thus not providing any feedback on whether a certain combination may be better than another.

In contrast to AHP and POSeM, MR-MOD's evaluation result is a set of Pareto-optimal portfolios out of all possible safeguard combinations that are not inferior to the others, i.e. non-dominated. It particularly addresses risk elements (assets, vulnerabilities, threats) and therefore any specific negative events that may occur. Like AHP, it is suitable for evaluating directly comparable security technologies such as virus scanners of different vendors, but it is also capable of comparing two incomparable security measures e.g. virus scanner with fire extinguisher by evaluating their performance in mitigating their specifically assigned risks. MR-MOD also takes multiple objectives into account when evaluating the safeguards, and there is a great flexibility in defining these categories with the use of the three different category types (risk, process, simple). Like POSeM, it uses process models as the basis for the elicitation of the elements worth to be protected (assets) and therefore accounts for the process-centered view of today's business. Unlike POSeM and AHP, it provides the decision makers with hard numbers representing the aggregated performance of the portfolio, which makes it easier to compare the Pareto-optimal solutions with each other. It is also possible to define certain restrictions regarding the aggregated values, e.g. resource constraints such as a limit for monetary costs of the portfolio. But this quantitative nature is also the main drawback of this methodology, its reliance on quantitative data. Many risk assessment frameworks are relying on qualitative input which is not as accurate as quantitative numbers, but circumventing the problem of the absence of required statistics such as threat occurrences. If that data is not available, it has to be estimated as accurately as possible; the MR-MOD case study has demonstrated the sensitivity of this framework on input data in certain circumstances. Because MR-MOD always evaluates all possible combination of safeguards, its performance depends heavily on the total number of candidates. As the number of possible combinations is equal to 2^n, the calculation time required by the MODStool software roughly doubles up with each new candidate. By imposing constraints on the composition of solutions (e.g. must-haves), the number of valid combinations can be reduced considerably, thus reducing the number of solutions to be tested for non-dominance and therefore decreasing the overall calculation duration. It also may be beneficial to break down the decision problem into several sub-problems e.g. by dividing the candidates into groups and to evaluate each group separately, therefore reducing the number of candidates for each evaluation session, and to synthesize the individual results afterwards to get the big picture. Both POSeM and AHP react far less elastic to additional candidates than MR-MOD.

8. Conclusion

8.1. Summary

Business processes are constantly exposed to security threats that may compromise the unimpeded execution of processes generating value. Therefore, it is of vital importance to protect the core processes against critical risks that may occur. But the definition of Secure Business Processes is coupled with several problems (cf. section 1.2) namely the lack of an integrated analysis of business processes with security-related issues, the multiobjective nature of the decision problem to select appropriate security safeguards, and the consideration of economical factors regarding these safeguards, i.e. maintaining their cost-effectiveness.

At first, this thesis has given some vital background information regarding business processes, information security, risk management, and multiobjective decision support. Then, some existing frameworks dealing with these concepts were introduced, including the popular decision support technique AHP, the security evaluation methodology based on process models POSeM, and established risk-based approaches such as CRAMM and OCTAVE. The main contribution of this thesis, the model-supported, risk-based multiobjective decision support framework MR-MOD, was introduced (cf. section 4), a methodology specifically developed to address the problems stated above.

Its main advantage over other approaches is the combination of multiple techniques and the inheritance of their strengths to overcome their individual weaknesses and shortcomings. While other techniques are focused on certain aspects of security only (measuring security level, proposing applicable safeguards, providing punctual technical solutions for specific problems), this methodology is aimed to be a holistic framework for the elicitation of security holes and the selection of appropriate methods to satisfy the security requirements. The individual strengths of this approach can be attributed to the incorporated concepts:

Process Modeling Using a process model for the elicitation of security requirements seems obvious, given the relative importance of business processes in today's process-centered business environment. When relying on process models as a starting point for a security crucial analysis of business activities, companies may focus on the core processes that are vital for generating value. The explicit graphical modeling of assets and threats helps in getting an overview of relevant entities. Especially for non-technical personnel such as members of the higher management level, the easy-to-understand Use Case modifications for threat modeling is useful to get a valuable insight into the otherwise technical domain of security analysis. This sensitizes them for security-related issues and possibly improves the efficiency in security investments.

Risk Assessment A structured security risk assessment process ensures the consideration of all possible threats and vulnerabilities, as well as the focus on the important things that matter, the valuable assets. Risk assessment techniques have been implemented with great success and make sure that due diligence is performed [Pel05]. The quantitative results of the risk assessment also facilitate the evaluation of candidate safeguards according to their risk-mitigating performance.

Workshop Structuring the risk assessment phase as a workshop allows for multiple persons to participate in the process. This is especially important as generally there is a lack of data required for a formal risk assessment, and often the experience and knowledge of domain experts are the only sources of information. By including multiple participants of different areas of the company, different preferences and opinions are considered to gain an almost complete view of the whole security situation of the business process.

Multiobjective Decision Support Using multiobjective decision making techniques is a logical step to address the multidisciplinary nature of the safeguard selection problem. Often it is not suitable to aggregate different dimensions to a single value and to rely solely on it to evaluate the alternatives. The multiobjective approach allows for the consideration of often conflicting factors that nevertheless are of major importance. This also enables companies to specify their own focus of the security assessment, reflecting their individual security policy. The outcome of this Pareto-dominance-based evaluation is a set of Pareto-optimal portfolios, in contrast to plain ranking techniques such as AHP.

The concept was implemented into the MODStool application, a Windows-based software tool that supports the MR-MOD process. Finally, MR-MOD was compared to AHP and POSeM to determine its strengths and weaknesses.

8.2. Research Questions Reviewed

In the following, the research questions specified in section 1.3 are reviewed to check whether these issues were answered:

- **How can the optimal combination of safeguards for a given business process be determined with respect to multiple objectives?** This thesis has listed some frameworks found in literature that are capable of dealing with some aspects of this question, but none was suitable to fully conform to that problem. Therefore, the main contribution of this thesis, the MR-MOD framework, was developed to determine the optimal safeguard portfolio given a business process with respect to multiple objectives.

- **Are multiobjective decision making techniques applicable for safeguard evaluation?** The MR-MOD framework has proven that the concept of Pareto-dominance is suitable for dealing with the multiobjective nature of the safeguard evaluation problem. This concept not only evaluates safeguards in different categories, but it also produces complete portfolio sets that are superior to all other possible combination.

- **Is it beneficial to combine multiobjective decision making and risk management methods to construct a holistic methodology for eliciting the needs for security and safeguards?** MR-MOD embodies a combination of risk assessment elements with multiobjective decision making techniques by using risk-related information and risk-mitigating effectiveness values of safeguards as decision categories. The feasibility of this concept was successfully demonstrated in the case study.

- **How can risks be identified using business process models?** The main risk elements, the assets exposed to threats, can be identified by analyzing business process models for asset participation. This includes the identification of tangible, as well as intangible assets. MR-MOD defines several asset types to improve the clarity of the process model and to aid in finding all relevant assets. Then the identified assets can be analyzed for any vulnerabilities, and hereafter, threats exploiting these vulnerabilities can be identified and modeled as well.

8.3. Further Work

Some issues with MR-MOD remain open for further work:

Quantitative Data MR-MOD requires a complete set of quantitative data for each defined entity, which may be problematic. Whereas data such as monetary values of tangible assets is easily elicited, e.g. by estimating their replacement costs, other numbers are harder to come by, such as the monetary value of company specific data, the exposure of certain vulnerabilities, and especially estimations on the probability of threats. While risk assessment is conducted in a workshop environment to alleviate this problem, the lack of quantitative data is still a major problem with this proposal.

Number of Candidates Because of the full iteration of all possible safeguard combinations, MR-MOD acts quite elastic to the number of candidates, and the duration of the calculation may be extremely high for large numbers of safeguards, as the total number of combinations is equal to 2^n. Breaking down the decision problem into multiple sub-problems or imposing constraints on the composition of the portfolios are two possible ways to keep the number of valid combinations on a manageable level.

A. Appendix

A.1. Business Process Modeling

"A model is basically a simplified abstract view of the complex reality" [Nor00]. A process model is "an abstract description of an actual or proposed process that represents selected process elements that are considered important to the purpose of the model and can be enacted by a human or machine" [CKO92]. In the business domain, a process model is an abstract representation of an actual business process (or a proposed business process) that usually includes various abstraction levels that are more or less detailed.

There are numerous different modeling techniques for developing accurate process models, ranging from the Role Activity Diagrams (RAD) [Oul95] and the Business Process Modeling Notation (BPMN) [OMG06] developed by the Business Process Management Initiative (BPMI)[1] to the Integrated DEFinition (IDEF)[2] [MPD92] family of methods or Petri Nets [MV00]. The modeling languages can be either graphically-based diagrams (as most of them are) or text-based (e.g. the XML-based Business Process Execution Language (BPEL)).

Modeling business processes can be a tedious work, so why bother with modeling at all? Using process models provides several benefits [BBSK06], [Moy05]:

Focus Using models as an abstract representation of the real world, it allows one to focus on the key aspects of the problem, ignoring unnecessary detail. This can be realized by developing different abstraction levels, each with a different focus.

Clarity Models identify and document the core business processes and provide a clear understanding of them, thus helping decision makers gain a valuable insight into the internal processes and related costs and required resources. Especially graphical representations such as diagrams can further enhance the perception of business processes for non-domain-experts.

[1] The BPMI merged with the Object Management Group (OMG) in 2005 and the BPMN is therefore maintained by the OMG since then and has been declared officially as an OMG standard in 2006.

[2] Formerly ICAM Definition Languages.

Responsiveness Using business process modeling (especially when in conjunction with an overall business management strategy) can speedup application modifications and business process adaption on demand and therefore enhances the responsiveness of business processes to market changes.

Business Flexibility Modeling provides process analysts with a tool for modifying and simulating processes on demand without changes in the actual processes. The simulation can be used for analyzing changes and the results can be the basis for further improvements.

Process models must contain a variety of information such as 'what is going to be done', 'who is doing it', and 'where and when is it done'. Curtis et al. define four different perspectives that reflect the different forms of information [CKO92], the modeling techniques usually refer to one or more of these:

Functional The functional perspective represents which process elements are performed and the relevant flows of informational entities.

Behavioral The behavioral perspective represents when and how process elements are performed (aspects like loops, iterations, sequencing, ...).

Organizational The organizational perspective represents where and by whom the process elements are performed and the physical communication mechanisms used, and the physical media and locations used for storing entities.

Informational The informational perspective represents the informational entities produced or manipulated in the processes, including data, artifacts, products, and objects.

Basically, diagrams can be distinguished into models that provide a dynamic view, representing the dynamic behavior of business processes (functional and behavioral perspectives), and a static view, dealing with static information (organizational and informational perspective).

Pidd defines five useful principles for effective modeling [Pid03][3]:

1. Model simple - think complicated
2. Be parsimonious, start small and add

[3] In [Mül05].

3. Divide and conquer, avoid mega-models

4. Use metaphors, analogies and similarities

5. Do not fall in love with data

Generally, modeling frameworks do not include mechanisms for expressing security issues. But some provide extension methods that can be used to add security semantics. The following section introduces three modeling frameworks, namely the Unified Modeling Language (UML), the Architecture of Integrated Information Systems (ARIS), and the Adonis Standard Application Library (ADO-STL), along with diagram types and corresponding elements. In contrast to single diagram type modeling methods (e.g. RAD), these integrated frameworks provide multiple diagram types, both dynamic and static, that give a more complete view of the business processes and related entities. The first two have been chosen because those are widely used, the latter one because it presents the basis for the development of the proposed methodology in this thesis. The descriptions include the model specifications as well as an examination of possible security extensions.

A.1.1. UML

The Unified Modeling Language (UML) is an object-oriented graphical modeling language and the de facto industry standard for software modeling [Kob99]. Started out as a collaboration among three methodologists collectively referred to as the 'three Amigos', Grady Booch, Ivar Jacobson, and James Rumbaugh, the UML was the result of endeavors to create a unified method of modeling. Together with a diverse mix of vendors and system integrators, now called the 'UML Partners', they improved the framework and proposed it to the Object Management Group (OMG), and in November 1997 the UML was officially adopted as its object modeling standard. The current version is 2.1.1 [OMG07a], [OMG07b].

The UML includes 13 different diagrams, divided into structure diagrams (Class Diagram, Component Diagram, Object Diagram, Composite Structure Diagram, Deployment Diagram, Package Diagram) and behavioral diagrams (Activity Diagram, Use Case Diagram, State Machine Diagram), representing the static and dynamic view respectively. Interaction diagrams (Sequence Diagram, Interaction Overview Diagram, Communication Diagram, Timing Diagram) are a subset of the behavioral diagrams. Figure A.1 shows the diagram hierarchy [OMG07b].

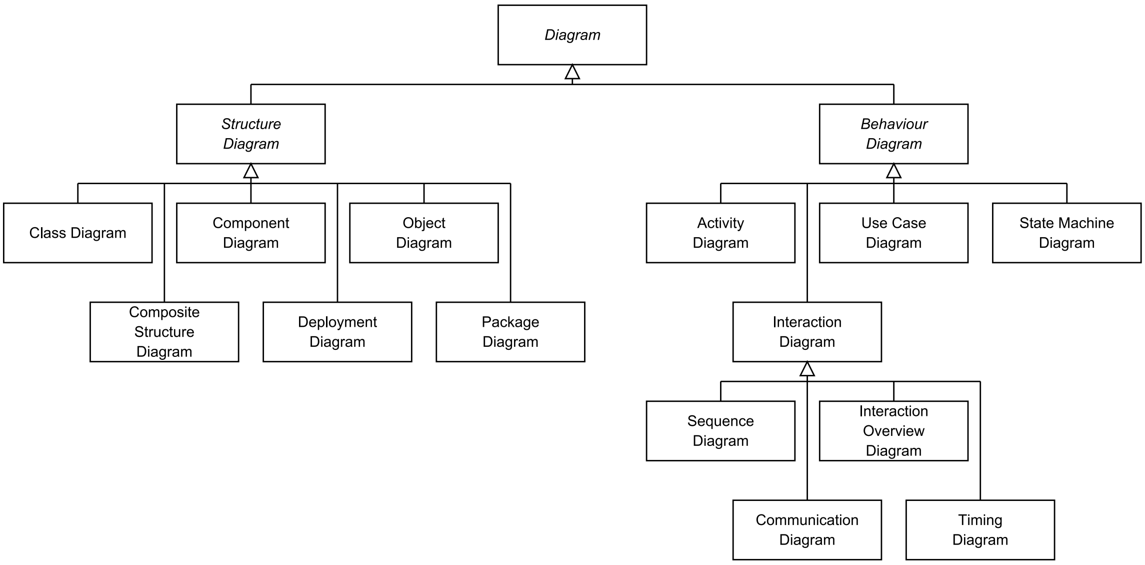


Figure A.1.: The Taxonomy of Structure and Behavior Diagrams

Aside from the numerous diagram types that can be used to model the different aspects of a system, UML additionally offers an extension mechanism: UML Profiles. A profile is a set of Stereotypes, Tagged Values, and Constraints, elements that can be used to adapt the UML semantics without changing the UML metamodel [OMG99]. As the UML metamodel is read only, profiles can only extend the existing elements and not insert new elements into the UML metamodel. Stereotypes are elements defined by their name and base class (base classes are usually metaclasses from the UML metamodel) and can have their own notation. Tagged values are name-value pairs that are assigned to stereotypes and can be used to express arbitrary information. Constraints are assigned to stereotypes as well and indicate restrictions. Constraints can be expressed in any language, or in a more specialized one, e.g. the Object Constraint Language (OCL), that is widely used [LK05].

The UML profiles can be used to specialize the UML metamodel to specific domains, a profile can be seen as a domain-specific interpretation of UML [OMG99]. Several researchers have published profiles for different purposes, notably business process modeling, e.g. [JEJ95], [Joh04], [SVC$^+$01], [LK05], [LK06].

This profile mechanism can be used to express security semantics as well. Some work has been done here, e.g. Jürjens introduces the UMLsec extension for secure systems development [Jür02], Rodriguez et al. define a UML 2 profile for modeling secure business processes [RFMP06], and Basin et al. develop a framework called Model-Driven

Security using their UML extension SecureUML [BDL06].

Apart from using specialized profiles for business process modeling, standard UML diagrams are capable of representing business processes as well. Usually, the following three diagrams, Use Case Diagrams[4], Activity Diagrams[4], and Class Diagrams[4]are used for this purpose.

Use Case Diagram

Use Case Diagrams are a part of the behavioral diagrams and specify the required usages of a system, i.e. what a system is supposed to do. They describe the behavior of a system from an external point of view and consist of the following elements: Actors are users and any other systems that interact with the system under consideration, and they are always model entities outside the system. They specify types of roles played by entities. Use Cases are specifications of sets of actions performed by a system. They express some behavior the system can perform but without giving any information about its internal structure. Extension Points are features of use cases and define where the behavior of use cases can be extended by elements of other use cases. The Subjects are the systems under considerations.

The Use Case Diagram elements apply the following relationships: Use relationships define which use cases are related to which actors. An actor can be assigned to multiple use cases, as well as a single use case to multiple actors. An Include relationship defines that the behavior of a specific use case (included use case) is inserted into the behavior of another specific use case (including use case). The including use case depends on the result of the execution of the included use case, and the latter is not optional but always a requirement for the correct execution of the including use case. An Extend relationship defines that the behavior of a specific use case (extending use case) can be extended by the behavior of another specific one (extended use case). This extended use case is specified independently of the extending one, and a single use case can extend multiple use cases. Figure A.2 shows an example of a Use Case Diagram [VP07].

Use Case Diagrams are suitable for displaying activities of business processes and participating actors on a high abstract level. This could be helpful in providing an overview of the business processes without going to much into detail, especially for non-domain experts that lack the specific domain knowledge.

[4] Information taken from [OMG07b].

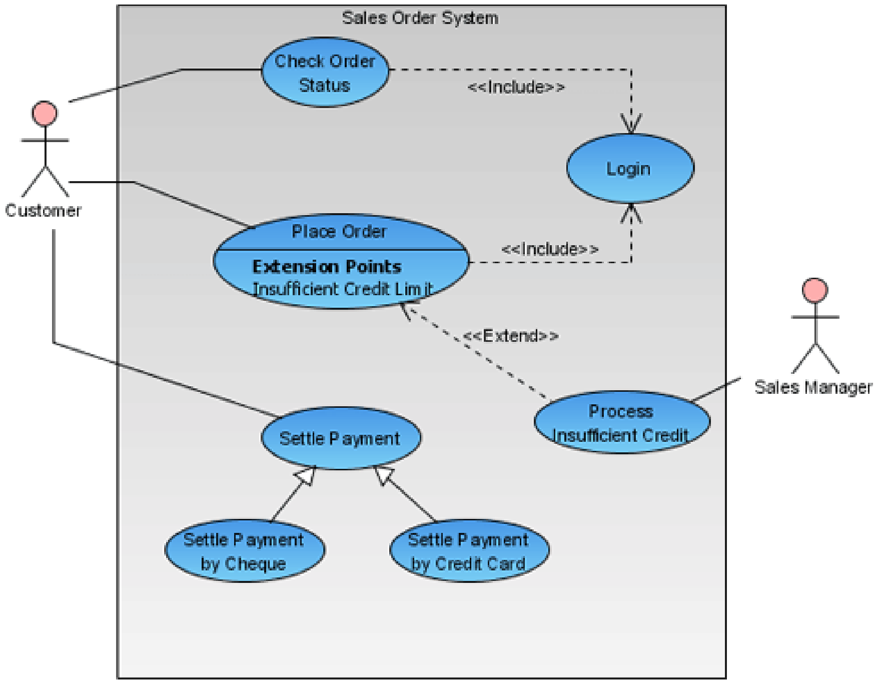


Figure A.2.: A sample Use Case Diagram

Activity Diagram - Dynamic View

Activity Diagrams describe the sequence and conditions for coordinating behavior. As a part of behavior diagrams, they provide information on the dynamic behavior of activities using control and object flow, thus giving a dynamic view of the system under consideration. The main elements of Activity Diagrams are as follows: Actions are the fundamental units of a system's behavior and represent a single step within an activity. They take a set of inputs and convert it into output. An action will not begin its execution if not all input conditions are met. Objects define instances of entities and include values that describe their states. They can be used in a variety of ways, depending on the information flow. Actions and objects are connected via ControlFlow and ObjectFlow edges respectively. Objects and data cannot flow via control flow edges.

Further elements are the so called Control Nodes: The InitialNodes specify the beginning of activities. There can be multiple InitialNodes within an activity. Analogously, ActivityFinalNodes define the ending and stop all flows. There can only be one ActivityFinalNode within an activity. FlowFinalNodes are similar nodes, but these only stop a particular flow, and there can be multiple FlowFinalNodes within an activity. ForkNodes split a flow into multiple concurrent flows; the opposites are JoinNodes, synchronizing multiple flows. DecisionNodes and MergeNodes specify a similar concept, but instead of splitting and synchronizing concurrent flows, they choose and accept one among several alternate flows.

Additional elements are the Containment Elements: Activities coordinate subordinate units and contain actions and objects. The opposites are ActivityPartitions that divide the elements within an activity and often represent organizational structures. Figure A.3 shows an Activity Diagram sample [VP07].

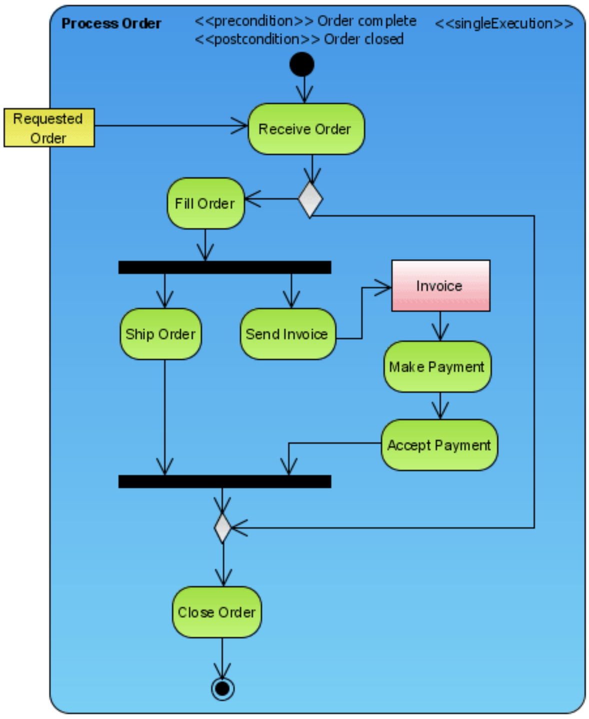


Figure A.3.: A sample Activity Diagram

Activity Diagrams are best used for modeling the particular flows within activities of business processes on a much lower abstraction level than use cases. They represent a method for developing detailed models of the internal behavior of business processes (how processes work), and the underlying activities can be analyzed for further improvements.

Class Diagram - Static View

Class Diagrams are a type of structure diagrams providing a static view of objects and classes inside systems and their relationships to each other. The purposes of Class Diagrams are diverse, e.g. domain-specific data structures. The main element is the Class, a description of objects that share the same specification of features, constraints, and semantics. Class specifications can contain Attributes (structure) and Operations (behavior). Interfaces define a set of common public features and obligations. Interfaces cannot be instantiated; they need to be implemented by an instantiable entity conforming to all interface specifications. Like classes, interfaces can be described by their attributes and operations. Sometimes, Packages are included in Class Diagrams, grouping elements and providing a namespace for the grouped elements.

Class Diagram objects can bear different relations to each other: Associations specify semantic relationships between instances of classes. Instances of associations are called Links. Aggregations are enumeration types that provide the literals for the kind of aggregation of a property. Compositions are special types of aggregations in that the composite objects take responsibility for the existence and storage of the composed objects (its parts). Dependencies are relationships that define some kind of dependency between model elements, i.e. an element (or a set of elements) requires other elements for specification or implementation. Realizations are similar to dependencies and specify the relationships between suppliers (serving as the specifications) and clients (implementation of the specifications). The InterfaceRealization relationship is a specialization of realizations where the supplier is an interface. And finally, the Generalization defines the relationship between a more general element and more specific elements, where the specific elements inherit the features of their 'parents'. Figure A.4 shows an example of Class Diagrams [VP07].

Class Diagrams can be utilized for modeling business processes, or more specifically their elements, from a static point of view. Emphasis lies on their internal structures and their relationships. Class Diagrams are especially suitable for modeling the assets of a business process (IT systems, resources, vital information, ...).

A.1.2. ARIS

The Architecture of Integrated Information Systems (ARIS) is an integrated framework for describing and modeling business processes and company structures developed by Scheer [Sch92], [Sch99], [Sch00]. In contrast to the object-oriented UML, ARIS is process-oriented and provides a holistic framework for the design, analysis, implementation, and optimization of business processes. As it was designed to present a complete picture of the processes (along with structural information), the result of the development process was a highly complex model. To reduce this complexity, two mechanisms were introduced: On the one hand, the overall context of a business process is divided into individual views that represent different modeling and design aspects. The use of

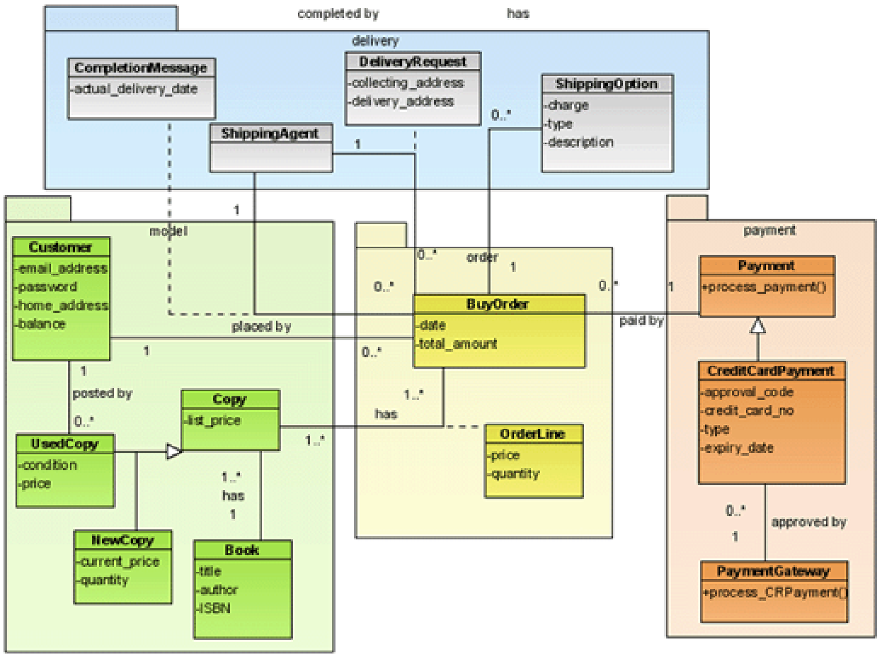


Figure A.4.: A sample Class Diagram

different views allows the description of individual views by particular methods without including the numerous relationships with other views. On the other hand, the views are analyzed on different descriptive levels. Different descriptive levels allow a consistent description of business management-related problems all the way down to their technical implementation.

The descriptive views comprise of the following five (cf. figure A.5) [IDS04]:

Organization Users and organizational units and their relationships are combined in the organization view.

Data The data view keeps track of changes in the state of information objects (data).

Function The functional view includes descriptions of the executed functions (processes), their subfunctions, and interrelationships.

Product/Service Products/Services represent the states in the (data) objects' environments and can be either concrete products or intangible services.

Control Breaking down the business process into individual views reduces the complexity, but also reduces information of relationships between the elements. Therefore, a fifth view, the control view, describes the relationships between the other views.

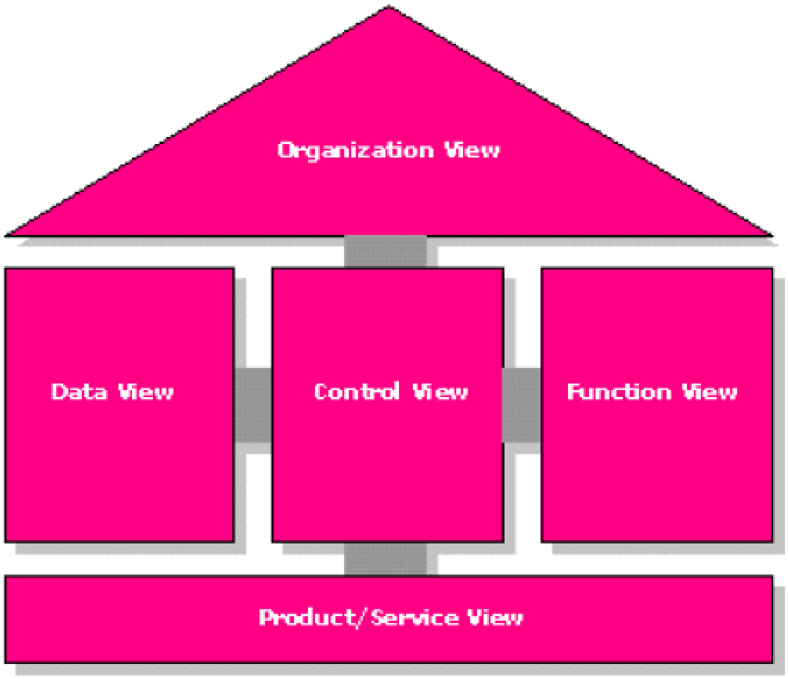


Figure A.5.: Descriptive Views of ARIS

The descriptive views are further structured into a three-tier descriptive level structure. An initial operational business problem serves as input for further analysis using the different views and levels. This problem is described using only semi-formal methods and lack detail. Then the following three descriptive levels are passed [IDS04]:

Requirements Definition The requirements definition is closely associated with the operational business problem and formally describes the business application (semantic modeling). That can be used as a starting point for a translation into information technology.

Design Specification In the design specification level, the business functions are replaced with executing modules or transactions, adapting the requirements descriptions to information technology. Although the design specification is only loosely coupled to the requirements definitions, it does not mean that both levels can be developed separately.

Implementation In the third step, the design specifications are carried over to concrete hardware and software components.

Figure A.6 shows descriptive views of the ARIS framework along with their corresponding descriptive levels and the operational business problem [IDS04].

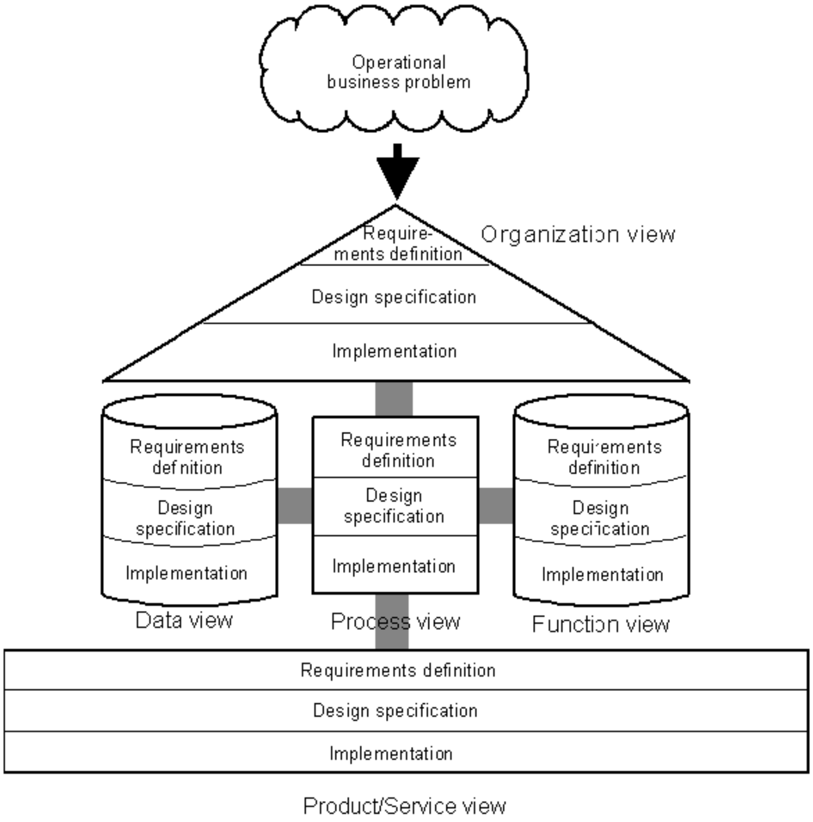


Figure A.6.: The ARIS Views with Descriptive Levels

The ARIS framework supports multiple diagram types for modeling the different views. Two of them are the Event-Driven Process Chains (EPC), representing the process view, and the Entity-Relationship Models (ERM), representing the data view. The framework does not provide any particular means for modeling security semantics and cannot be adapted as easily as UML. Nevertheless, ARIS has been under consideration for being extended with security-related issues, albeit not that exhaustive: Mock and Corvo integrate ARIS and the Failure Mode and Effects Analysis (FMEA) [MC05]. Specifically, the functions of EPCs are examined for failure modes and the diagrams are extended with elements representing the latter. Zur Mühlen and Rosemann present a taxonomy of process-related risks and demonstrate how a modeling method can be extended to express risks of business processes [zMR05]. They propose an extension of the ARIS framework with four model types: Risk Structure model, Risk Goal model, Risk State model, and EPCs extended with risks. EPCs and elements of the ERMs are used for developing the additional models, although some authors claim that ERMs are not suited for expressing security semantics [KDK00].

In the following, EPCs[5] and ERMs[6] are described.

Event-Driven Process Chains - Dynamic View

Event-Driven Process Chains (EPC) are an integral part of the ARIS framework for modeling the process view (at the requirements definition level) providing a dynamic view of the business process. They have been developed by Scheer in the context of the development of the ARIS framework and are widely used. The main elements of the EPCs are Functions and Events. Functions are activities within a business process and represent the active components of the diagram that consume time. They can be aggregated or further divided. Events are states within a business process and represent the passive components that are related to one point in time. They trigger functions and are the results of functions. Semantically, functions may only be preceded and succeeded by events and vice versa. Starting and ending nodes are only events.

Functions and events are connected via different types of function and event operators (depending on the element). The simplest connection type is the vectored edge. All other types include some sort of branching: The AND operator states that all forked (or joined) functions/events are valid for the process flow. The OR operator states that at least one of the forked (or joined) functions/events is valid. And finally, the XOR operator states that only one of the forked (or joined) functions/events are chosen. Some semantical restrictions need to be considered as events cannot make decisions and therefore a triggering event must not be linked using an OR or XOR operator. Figure A.7 shows a sample EPC diagram [IDS04].

EPCs may be extended with Organizational elements and Input/Output allocation data, resulting in the Extended Event-Driven Process Chains (eEPC). Organizational elements represent the task performers that are assigned to the functions and serve as a link between the function view and the organizational view modeled in the process view. Input/Output allocation data are information objects and represent the link between the function and data view. Arrows indicate whether an information object serves as input or output.

[5] Information taken from [IDS04].

[6] Information taken from [IDS04] and [Bal96].

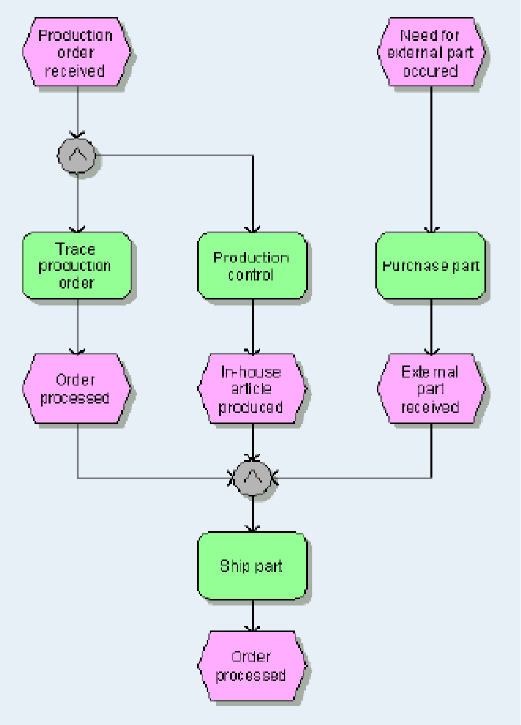


Figure A.7.: A sample EPC Diagram

Entity-Relationship Model - Static View

The basic Entity-Relationship Model (ERM) developed by Chen [Che76] is a language for semantic data modeling. It is a popular method for modeling the data view in the ARIS framework and provides a static view of the system. The main elements of an ERM are the Entities that are objects of the environment or objects specifying events. They can be further described by assigning Attributes to them. Attributes are properties of entities and all entities of the same type possess the same attributes (entity set). Attributes can either be descriptive or identifying, the latter can be used as keys. Keys can either be a single or a combination of multiple identifying attributes. Attributes can never have attributes themselves; an attribute that has an attribute becomes an entity.

Entities are connected via relationships. These relationships are labeled connection types that are distinguished by their cardinality that defines the numbers of entity types linked to them: The 1:1 relationship defines that each entity of the first set is precisely related to an entity of the second set. The 1:n and n:1 relationships define that each entity of the first set can be linked to n entities of the second set or the other way round. The n:m relationship defines that n entities of the first set can be assigned to m entities of the second set.

All these relationship types represent a must-relation. Can-relations are modeled with the conditional relationship types, e.g. the 1:c relationship defines that each entity of the first set may be related to either one or none entity of the second set, but an entity of the second must be assigned to one of the first set. The other conditional types are c:1, 1:nc, nc:1, c:c, n:c, c:n, mc:n, m:nc, nc:c, c:nc, and mc:nc.

Entities may be related to themselves; the resulting relationships are called recursive (all cardinality types can be applied).

In order to become an appropriate method for semantic data modeling, the ERM was extended by multiple authors resulting in the Extended Entity-Relationship Model (eERM). Two important additions to the basic ERM are the concepts of Aggregation and Generalization. An aggregation is a special relationship that defines a part-of-relation, i.e. subordinated entities are part of the superordinated entities. Cardinalities are applied as with the other associations. A generalization defines an is-a-relation, i.e. subordinated entities (subtype) inherit the attributes (along with the key) of superordinated entities (supertypes), but have their own attributes as well. The generalization operation is applied to the entity set (in contrast to the other relationship types that are applied to entities). Figure A.8 shows a sample ERM.

A.1.3. ADONIS Standard Application Library

The ADONIS Standard Application Library (ADO-STL) is a business process modeling language and part of the proprietary Adonis® Business Process Management Toolkit by BOC[7]. The Adonis toolkit is an integrated framework that provides functions for the acquisition, modeling, analysis, simulation, and documentation of business process models and is part of BOC Management Office® (along with the Strategy and Performance Management tool ADO*score*®, the Supply Chain Design tool ADO*log*®, and the IT Architecture and Service Management tool ADO*it*®). The version used in this thesis is 3.81.

By default, the Adonis toolkit is shipped with the ADO-STL with 5 predefined model types: Process Map, Business Process Model, Working Environment Model, Document Model, and Use Case Diagram (figure A.9, adapted from [BOC04]). On demand, BOC also includes the toolkit with additional international standard methods and notations such as UML, BPMN, EPC, or LOVEM. The object-oriented meta-modeling concept

[7] www.boc-eu.com

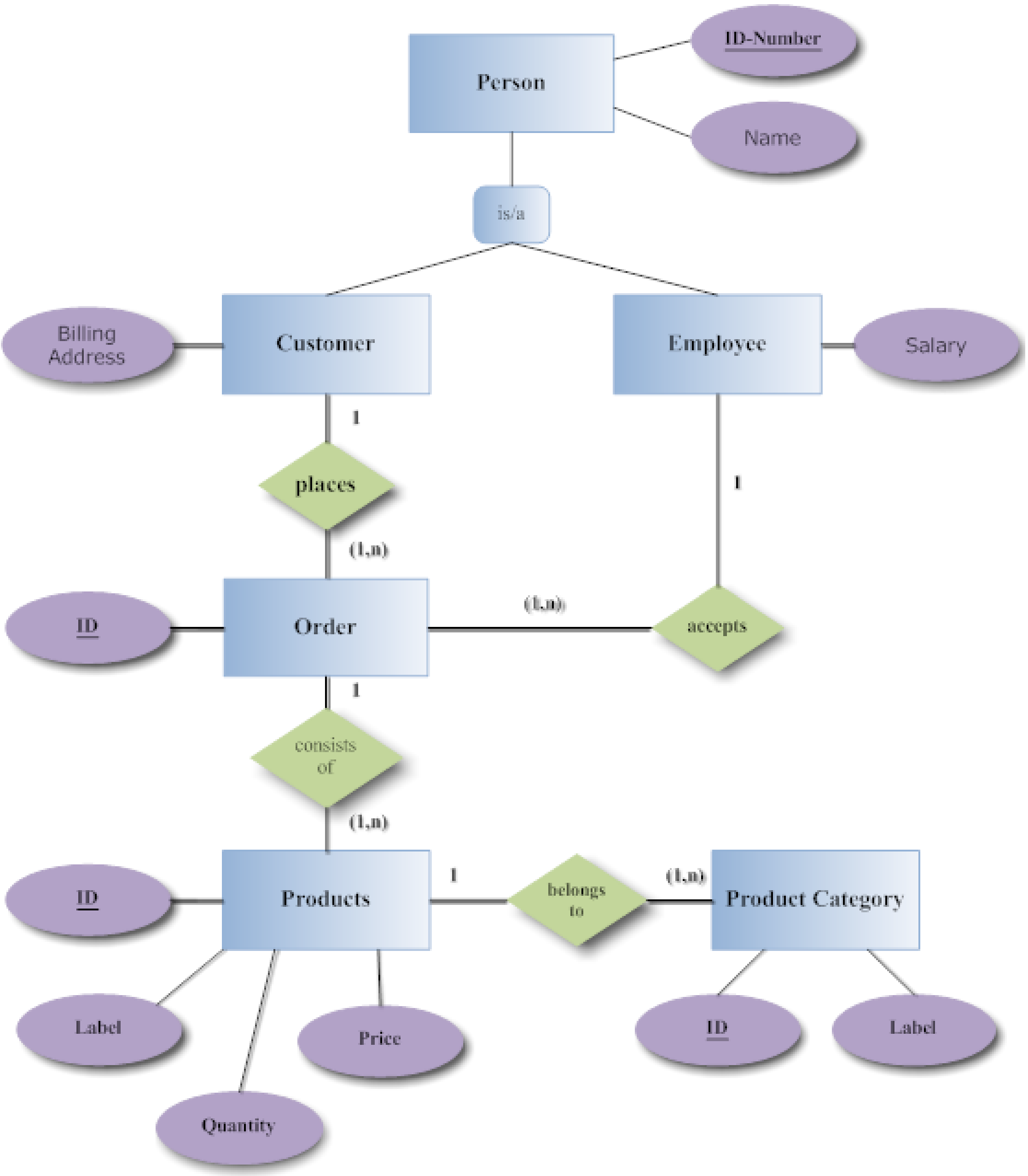


Figure A.8.: A sample ERM Diagram

within the Adonis framework allows the adaption of the toolkit for domain specific modeling tasks. An administration tool provides measures for the development of additional model types and the modification of classes (model elements and class attributes).

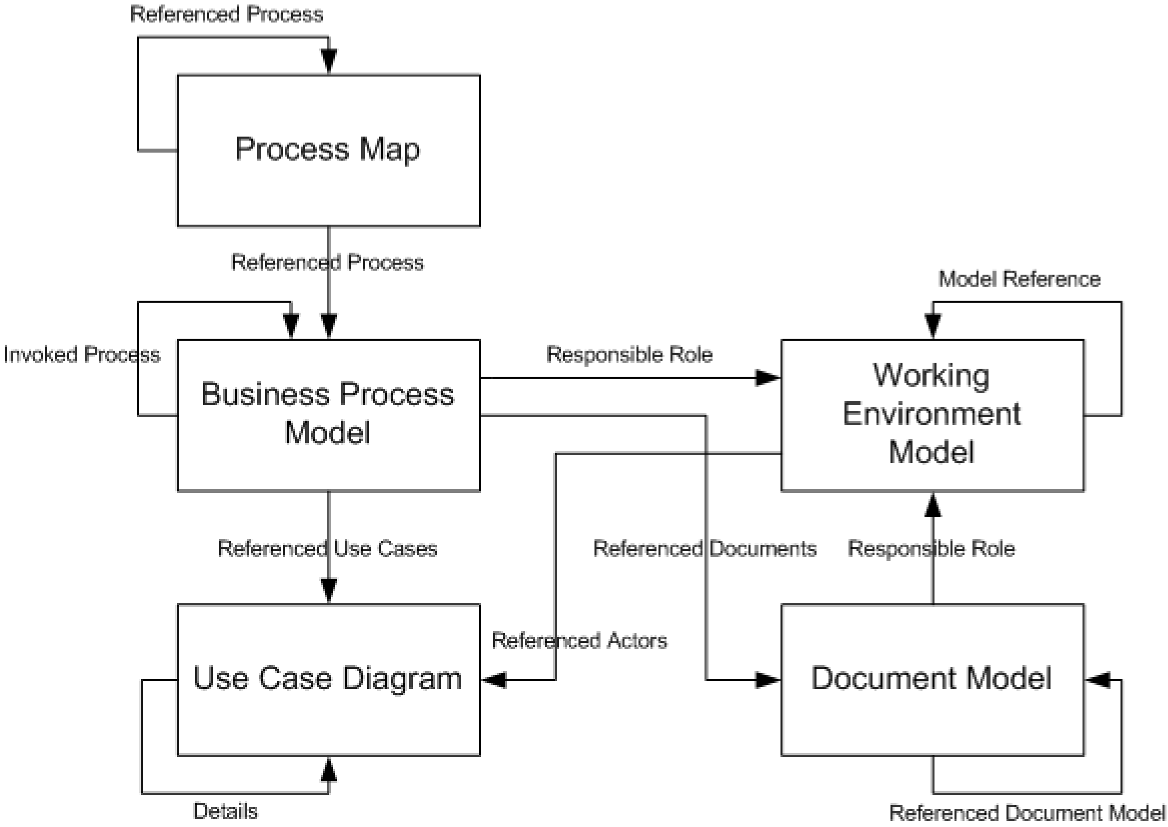


Figure A.9.: Adonis Model Types

Like ARIS, the Adonis framework and the ADO-STL do not support the explicit modeling of security semantics. The meta-model adaption concept of the framework, however, can be utilized to develop means for expressing security-related information. The addition of security-related model types is part of the proposed methodology of this thesis.

In the following, the five standard model types[8] of the ADO-STL are introduced.

Process Map

The Process Map provides an overview of Business Process Models or other Process Maps. It can be used as a navigational help or as an entry point for the Business

[8] Information taken from [BOC04].

Process Model hierarchy. The Process Map includes the following elements (classes): A Process represents a business process and is a reference to Business Process Models. The Note element can be used to include additional documentation. The Aggregation element is used to aggregate single elements to groups.

For the Process Map, the relationships Has Process and Has Note which represent the connections between process maps and notes are defined. Figure A.10 shows a sample Process Map.

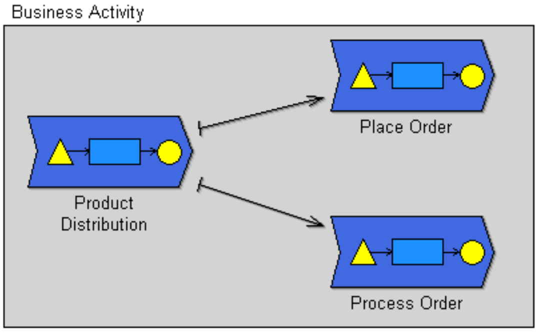


Figure A.10.: A sample Process Map Diagram

Business Process Model - Dynamic View

The Business Process Model is the central part of the ADO-STL and represents the processes within an organization. The main elements are the Activities that describe the tasks a process is comprised of. Activities are controlled by the following control objects: The Process Start is the starting point of each process and there can only be one process start element within each Business Process Model. The Subprocess element is used to model a referenced process and helps to improve the readability and structure of a Business Process Model. A Decision element allows the query of predefined Variables and Variable Values and the corresponding choice of a particular flow path. The Parallelity and Merging elements are forking mechanisms and allow the splitting and merging of multiple independent, but simultaneously executed, parts of the process. End objects define the ends of flow paths (unlike process start elements, there can be multiple end objects within a process). Further elements are the Resources, the Performance Indicators (and Overview), Notes, and the Aggregation.

The following connection types are specified for the Business Process Model: Successors links activities, Occupies and Occupies Variable link variables and activities, Uses links activities and resources, Owns links activities and performance indicators, and Has Notes links notes to all other elements. Figure A.11 shows a sample Business Process Model.

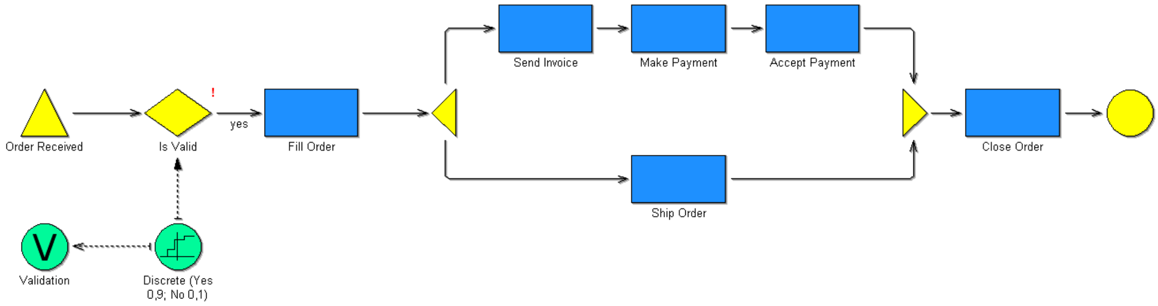


Figure A.11.: A sample Business Process Model Diagram

Working Environment Model - Static View

The Working Environment Model models the structure of an organization, where the following elements are defined: The Organizational Unit is the central element of the diagram and allows the clear modeling of the working environment hierarchy. Multiple Performers that execute tasks are assigned to organizational units; the same performer can be assigned to multiple organizational units. Performers have one or more Roles that specify their fields of duty. Again, the same role can be assigned to multiple performers. Additional elements are Resources and Cost centers (both used in the simulation), and Notes and Aggregation.

The following connection types are used in the Working Environment Model: Is Superordinated defines the hierarchy of organizational units, Belongs To assigns performers to organizational units, Is Leader specifies a team leader, Has Role assigns roles to performers, and Has Resource, Uses Resource, Is Added, and Is Cost Center Leader are used in conjunction with resources and cost centers. Has Notes links notes to all other elements. Figure A.12 shows a sample Working Environment Model.

Document Model - Static View

The Document Model is a simple diagram that contains all necessary documents for the execution of the processes. The main elements are the Documents. Documents contain information and support the execution of activities. They are referenced from

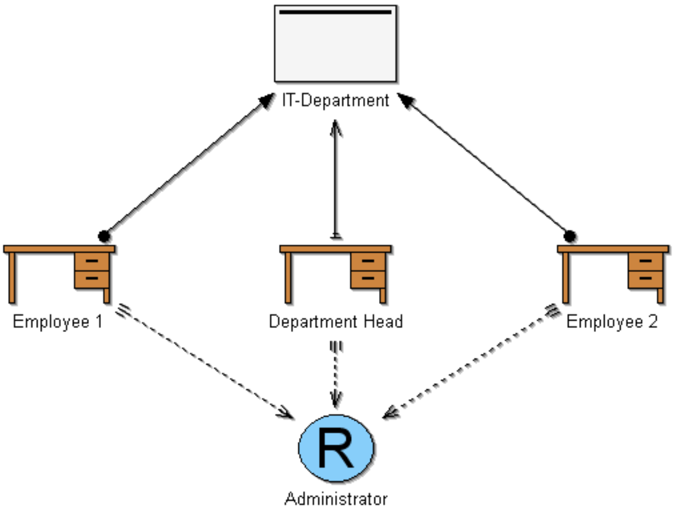


Figure A.12.: A sample Working Environment Model Diagram

the activities of the Business Process Model. Again, the elements Notes and Aggregation are included in this diagram.

The only connection types are Has Notes and Has Subdocument, the latter defining the hierarchy of documents. Figure A.13 shows a sample Document Model.

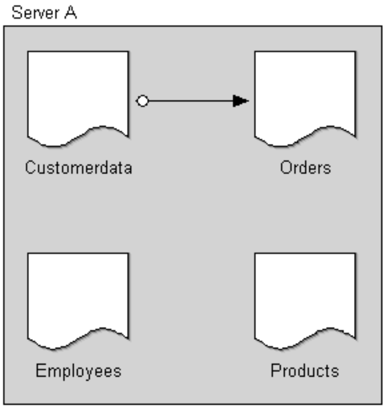


Figure A.13.: A sample Document Model Diagram

Use Case Diagram

The Use Case Diagrams are basically the same as specified within the UML framework, but with the element Notes and the connection type Has Notes.

A.2. Case Study Data

Table A.1.: Risks and Mitigating Control Groups

Risk	**Asset**	**Threat**	**Vulnerability**	**Control**
Burst of Fire	DB Server	Fire	No Fire Suppression Control	FSC
Burst of Fire	App. Server	Fire	No Fire Suppression Control	FSC
Burst of Fire	Workstation	Fire	No Fire Suppression Control	FSC
Data Loss due to Fire	Request Data	Fire	No Fire Suppression Control	FSC
Data Loss due to Fire	Request DB	Fire	No Fire Suppression Control	FSC
Data Loss due to Fire	Applicant Data	Fire	No Fire Suppression Control	FSC
Data Loss due to Fire	Money Order Data	Fire	No Fire Suppression Control	FSC
Hardware Issues	DB Server	Hardware Failure	No Hardware Maintenance / No Fallback Equipment	MFC
Hardware Issues	App. Server	Hardware Failure	No Hardware Maintenance / No Fallback Equipment	MFC
Hardware Issues	Workstation	Hardware Failure	No Hardware Maintenance / No Fallback Equipment	MFC
Hardware Issues	Network	Hardware Failure	No Hardware Maintenance / No Fallback Equipment	MFC
Data Loss due to HW Failure	Request Data	Hardware Failure	No Hardware Maintenance / No Fallback Equipment	MFC
Data Loss due to HW Failure	Request DB	Hardware Failure	No Hardware Maintenance / No Fallback Equipment	MFC
Data Loss due to HW Failure	Applicant Data	Hardware Failure	No Hardware Maintenance / No Fallback Equipment	MFC
Data Loss due to HW Failure	Money Order Data	Hardware Failure	No Hardware Maintenance / No Fallback Equipment	MFC
Malware Infection	DB Server	Malware Upload	No Virus Scanner / No Regular Updates	AVC, RUC
Malware Infection	App. Server	Malware Upload	No Virus Scanner / No Regular Updates	AVC, RUC
Malware Infection	Workstation	Malware Upload	No Virus Scanner / No Regular Updates	AVC, RUC
Unwanted Tampering with Software	Scanning SW.	Malware Upload	No Virus Scanner / No Regular Updates	AVC, RUC
Unwanted Tampering with Software	Checking SW.	Malware Upload	No Virus Scanner / No Regular Updates	AVC, RUC
Unwanted Tampering with Software	COTS DMS	Malware Upload	No Virus Scanner / No Regular Updates	AVC, RUC
Loss of Data Conf.	Request Data	Malware Upload	No Virus Scanner / No Regular Updates	AVC, RUC
Loss of Data Conf.	Request DB	Malware Upload	No Virus Scanner / No Regular Updates	AVC, RUC
Loss of Data Conf.	Applicant Data	Malware Upload	No Virus Scanner / No Regular Updates	AVC, RUC
Loss of Data Conf.	Money Order Data	Malware Upload	No Virus Scanner / No Regular Updates	AVC, RUC

Table A.2.: Risks and Mitigating Control Groups - Cont.

Risk	**Asset**	**Threat**	**Vulnerability**	**Control**
Impersonation	Workstation	Impersonation	No proper Access Policy	ACC
External Data Theft / Manipulation	Request Data	Ext. Data Theft	No proper Access Policy	ACC
External Data Theft / Manipulation	Request DB	Ext. Data Theft	No proper Access Policy	ACC
External Data Theft / Manipulation	Applicant Data	Ext. Data Theft	No proper Access Policy	ACC
External Data Theft / Manipulation	Money Order Data	Ext. Data Theft	No proper Access Policy	ACC
Internal Data Manipulation	Request Data	Data Manipulation	No proper Access Policy	ACC
Internal Data Manipulation	Request DB	Data Manipulation	No proper Access Policy	ACC
Internal Data Manipulation	Applicant Data	Data Manipulation	No proper Access Policy	ACC
Internal Data Manipulation	Money Order Data	Data Manipulation	No proper Access Policy	ACC
Unwanted Money Transfers	Webservice	Impersonation	No proper Access Policy	ACC
Network Eavesdropping	Network	Eavesdropping	Lack of Encryption Techniques	ECC
Eavesdropping of Mails	E-Mail-system	Eavesdropping	Lack of Encryption Techniques	ECC
Eavesdropping of Money Transfers	Webservice	Eavesdropping	Lack of Encryption Techniques	ECC
Unwanted Money Transfers	Webservice	Impersonation	Lack of Encryption Techniques	ECC
Sabotage by internal Threat Agent	DB Server	Hardware Sabotage	Lack of physical Protection Mechanisms	PPC
Sabotage by internal Threat Agent	App. Server	Hardware Sabotage	Lack of physical Protection Mechanisms	PPC
Sabotage by internal Threat Agent	Workstation	Hardware Sabotage	Lack of physical Protection Mechanisms	PPC
Sabotage by internal Threat Agent	Network	Hardware Sabotage	Lack of physical Protection Mechanisms	PPC
Data Loss due to Hardware Sabotage	Request Data	Hardware Sabotage	Lack of physical Protection Mechanisms	PPC
Data Loss due to Hardware Sabotage	Request DB	Hardware Sabotage	Lack of physical Protection Mechanisms	PPC
Data Loss due to Hardware Sabotage	Applicant Data	Hardware Sabotage	Lack of physical Protection Mechanisms	PPC
Data Loss due to Hardware Sabotage	Money Order Data	Hardware Sabotage	Lack of physical Protection Mechanisms	PPC
Data Entry Error	Scanning SW	Data Entry Error	Carelessness	ETC
Data Entry Error	Checking SW	Data Entry Error	Carelessness	ETC
Data Entry Error	COTS DMS	Data Entry Error	Carelessness	ETC
Error Overlooking	Scanning SW	Error Overlooking	Carelessness	ETC
Error Overlooking	Checking SW	Error Overlooking	Carelessness	ETC
Error Overlooking	COTS DMS	Error Overlooking	Carelessness	ETC

Table A.3.: Risks and Mitigating Control Groups - Cont.

Risk	Asset	Threat	Vulnerability	Control
Unwanted Tampering with Software	Scanning SW	Malware Upload	Lack of Security Awareness / IT Training	ETC
Unwanted Tampering with Software	Checking SW	Malware Upload	Lack of Security Awareness / IT Training	ETC
Unwanted Tampering with Software	COTS DMS	Malware Upload	Lack of Security Awareness / IT Training	ETC
Offline Industrial Espionage	Request Data	Social Engineering	Lack of Security Awareness / IT Training	ETC
Offline Industrial Espionage	Request DB	Social Engineering	Lack of Security Awareness / IT Training	ETC
Offline Industrial Espionage	Applicant Data	Social Engineering	Lack of Security Awareness / IT Training	ETC
Inconsistent Money Order Data	Money Order Data	Internet Connection Breakdown	No or Insufficient Logging	SLC
E-Mail Problems	E-Mail System	Internet Connection Breakdown	No or Insufficient Logging	SLC
Repudiation of Money Transfers	Webservice	Internet Connection Breakdown	No or Insufficient Logging	SLC
Data Loss due to Power Failure	Request Data	Power Failure	No proper Backup Strategy	BSC
Data Loss due to Power Failure	Request DB	Power Failure	No proper Backup Strategy	BSC
Data Loss due to Power Failure	Applicant Data	Power Failure	No proper Backup Strategy	BSC
Data Loss due to Power Failure	Money Order Data	Power Failure	No proper Backup Strategy	BSC
Intrusion into System	DB Server	Intrusion	No Network Protection	FWC
Intrusion into System	App. Server	Intrusion	No Network Protection	FWC
Network Eavesdropping	Network	Eavesdropping	No Network Protection	FWC
External Data Theft / Manipulation	Request Data	Ext. Data Theft	No Network Protection	FWC
External Data Theft / Manipulation	Request DB	Ext. Data Theft	No Network Protection	FWC
External Data Theft / Manipulation	Applicant Data	Ext. Data Theft	No Network Protection	FWC
External Data Theft / Manipulation	Money Order Data	Ext. Data Theft	No Network Protection	FWC

Table A.4.: Asset Values and Process Impact Values

Asset	Asset Value Pr.	Sec. Status	Proc. Benefit	Prod. Loss
Database Server	15000	4*8*6 = 192	100	100
Application Server	15000	4*8*6 = 192	90	90
Workstation	5000	2*6*4 = 48	50	50
Network Infrastructure	25000	4*8*6 = 192	100	100
Scanning Software	15000	6*8*6 = 288	90	90
Checking Software	15000	6*8*6 = 288	90	90
COTS DMS	8500	2*6*6 = 72	90	90
Request Data	5000	8*8*6 = 384	100	100
Request Database	25000	8*8*6 = 384	100	100
Applicant Insurance Status Data	5000	8*8*6 = 384	100	100
Money Order Data	10000	10*10*6 = 600	100	100
E-Mail-System	3500	6*8*6 = 288	30	30
Ext. Webservice	50000	10*10*6 = 600	100	100

Table A.5.: Vulnerability Exposure Factors

Vulnerability	**Asset Value Preservation**	**Security Status**
No proper Backup Strategy	100	100
Lack of Security Awareness / IT Training	5	45
No Network Protection	50	90
No Virus Scanner / No Regular Updates	15	90
No Hardware Maintenance / No Fallback Equipment	60	45
No proper Access Restriction Policy	55	100
Lack of Encryption Techniques	80	80
No Fire Suppression Control	90	70
Lack of physical Protection Mechanisms	60	60
No or insufficient Logging	40	75
Carelessness	5	15

Table A.6.: Threat AROs

Threat	**Annual Rate of Occurrence**
Data Entry Error	200
Error Overlooking	100
Fire	0.1
Power Failure	5
Internet Connection Breakdown	20
Hardware Failure	2
Malware Upload	150
Eavesdropping	20
Intrusion	20
External Data Theft or Manipulation	5
Impersonation	2
Hardware Sabotage	0.5
Unauthorized Data Manipulation	5
Social Engineering	3

Table A.7.: Simple Safeguard Values

Safeguard	**User Acceptance**	**Setup Costs**	**Running Costs**	**Maintenance**
Backup A	90	0	500	120
Backup B	85	6000	1500	200
Backup C	80	7000	3000	260
Backup D	60	7500	4000	360
Regular Equipment Maint.	70	0	1000	100
Basic Fallback Equipment	75	5000	1100	120
Full Fallback Equipment	80	30000	1300	140
Weekly Updates	90	0	500	10
Daily Updates	85	0	2500	50
Virus Scanner A	95	0	0	10
Virus Scanner B	90	500	100	25
Virus Scanner C	95	550	120	20
SK Encryption	80	2500	500	80
PK Encryption	80	3000	1500	90
Firewall A	75	0	0	15
Firewall B	80	600	150	10
Firewall C	55	550	50	25
Firewall D	90	1000	150	30
Firewall E	60	700	350	50
Fault Logging	70	0	500	100
Full Logging	60	0	600	200
Port. Fire Ext.	80	1000	200	10
Fixed Fire Ext.	85	20000	2500	95
Physical Locks	60	500	100	5
Surveillance System	30	10000	2000	250
Security Guards	25	10000	7500	250
Basic Training	40	0	5000	50
Ext. Training	20	0	15000	100
User Rights Restr.	40	1500	5000	75
Enh. Password Policy	35	2000	2500	55

Table A.8.: Process-related Safeguard Effectiveness (Process Benefit)

Safeguard	**DBS**	**APS**	**WS**	**NI**	**SS**	**CS**	**DMS**	**RD**	**RDB**	**AD**	**EMS**	**WS**	**MOD**
Backup A	x	x	x	x	x	x	x	85	85	85	x	x	85
Backup B	x	x	x	x	x	x	x	95	95	95	x	x	95
Backup C	x	x	x	x	x	x	x	95	95	95	x	x	95
Backup D	x	x	x	x	x	x	x	100	100	100	x	x	100
Reg. Maint.	35	45	50	55	x	x	x	35	35	35	x	x	35
Basic Fallb.	35	35	20	25	x	x	x	40	40	40	x	x	40
Full Fallb.	65	55	50	45	x	x	x	65	65	65	x	x	65
Weekly Upd.	35	35	50	x	40	40	50	50	35	50	x	x	50
Daily Upd.	35	35	75	x	60	60	65	75	65	75	x	x	75
Scanner A	70	70	85	x	70	70	75	55	55	55	x	x	35
Scanner B	85	80	90	x	80	80	85	75	75	75	x	x	75
Scanner C	75	25	95	x	95	95	95	60	60	60	x	x	60
SK Encryp.	x	x	x	85	x	x	x	x	x	x	85	85	x
PK Encryp.	x	x	x	95	x	x	x	x	x	x	95	95	x
Firewall A	70	80	x	75	x	x	x	0	0	0	x	x	0
Firewall B	80	75	x	75	x	x	x	0	0	0	x	x	0
Firewall C	90	95	x	90	x	x	x	0	0	0	x	x	0
Firewall D	60	75	x	70	x	x	x	0	0	0	x	x	0
Firewall E	80	80	x	80	x	x	x	0	0	0	x	x	0
Fault Log.	x	x	x	x	x	x	x	x	x	x	25	65	65
Full Log.	x	x	x	x	x	x	x	x	x	x	45	80	80
Port. FE	80	80	75	x	x	x	x	80	80	90	x	x	80
Fixed FE	95	95	95	x	x	x	x	95	95	95	x	x	95
Phys. Locks	70	75	40	30	x	x	x	0	0	0	x	x	0
Surv. Sys.	90	90	90	35	x	x	x	0	0	0	x	x	0
Sec. Guards	95	95	95	40	x	x	x	0	0	0	x	x	0
Basic Train.	x	x	x	x	20	25	40	40	40	40	x	x	x
Ext. Train.	x	x	x	x	40	35	50	65	65	65	x	x	x
User RR	x	x	80	x	x	x	x	85	85	85	x	95	85
Enh. PP	x	x	85	x	x	x	x	85	85	85	x	85	85

Table A.9.: Process-related Safeguard Effectiveness (Productivity Loss)

Safeguard	**DBS**	**APS**	**WS**	**NI**	**SS**	**CS**	**DMS**	**RD**	**RDB**	**AD**	**EMS**	**WS**	**MOD**
Backup A	x	x	x	x	x	x	x	0	0	0	x	x	0
Backup B	x	x	x	x	x	x	x	0	0	0	x	x	0
Backup C	x	x	x	x	x	x	x	0	0	0	x	x	0
Backup D	x	x	x	x	x	x	x	0	0	0	x	x	0
Reg. Maint.	10	10	25	35	x	x	x	0	0	0	x	x	0
Basic Fallb.	10	10	25	35	x	x	x	0	0	0	x	x	0
Full Fallb.	10	10	25	35	x	x	x	0	0	0	x	x	0
Weekly Upd.	5	5	10	x	0	0	0	0	0	0	x	x	0
Daily Upd.	10	10	15	x	0	0	0	0	0	0	x	x	0
Scanner A	25	25	45	x	5	5	5	35	35	35	x	x	35
Scanner B	20	35	35	x	5	5	5	55	55	55	x	x	55
Scanner C	25	20	45	x	5	5	5	45	45	45	x	x	45
SK Encryp.	x	x	x	15	x	x	x	x	x	x	35	20	x
PK Encryp.	x	x	x	20	x	x	x	x	x	x	55	35	x
Firewall A	10	10	x	20	x	x	x	0	0	0	x	x	0
Firewall B	15	5	x	25	x	x	x	0	0	0	x	x	0
Firewall C	8	10	x	35	x	x	x	0	0	0	x	x	0
Firewall D	10	15	x	15	x	x	x	0	0	0	x	x	0
Firewall E	25	20	x	20	x	x	x	0	0	0	x	x	0
Fault Log.	x	x	x	x	x	x	x	x	x	x	0	5	5
Full Log.	x	x	x	x	x	x	x	x	x	x	5	10	10
Port. FE	0	0	0	x	x	x	x	0	0	0	x	x	0
Fixed FE	0	0	0	x	x	x	x	0	0	0	x	x	0
Phys. Locks	5	5	5	5	x	x	x	0	0	0	x	x	0
Surv. Sys.	15	15	10	10	x	x	x	0	0	0	x	x	0
Sec. Guards	15	15	10	10	x	x	x	0	0	0	x	x	0
Basic Train.	x	x	x	x	25	25	25	15	15	15	x	x	x
Ext. Train.	x	x	x	x	45	45	45	25	25	25	x	x	x
User RR	x	x	25	x	x	x	x	30	30	30	x	10	30
Enh. PP	x	x	25	x	x	x	x	30	30	30	x	5	30

Table A.10.: Risk-related FSC Effectiveness (Asset Value Pres. / Security Status)

Risk	**Portable Fire Ext.**	**Fixed Fire Extinguisher**
Burst of Fire DBS	80/30	95/35
Burst of Fire AS	80/30	95/35
Burst of Fire WC	75/25	95/35
Data Loss due to Fire RD	80/30	95/35
Data Loss due to Fire RDB	80/30	95/35
Data Loss due to Fire AD	80/30	95/35
Data Loss due to Fire MOD	80/30	95/35

Table A.11.: Risk-related MFC Effectiveness (Asset Value Pres. / Security Status)

Risk	**Reg. Equip. Maint.**	**Basic Fallback Set**	**Full Fallback Set**
Hardware Issues DBS	40/10	25/5	60/25
Hardware Issues AS	35/10	35/10	65/25
Hardware Issues WS	55/10	25/10	45/25
Hardware Issues NI	55/10	25/10	45/25
Data Loss due to Hardware Failure RD	55/10	25/10	45/25
Data Loss due to Hardware Failure RDB	40/10	25/5	60/25
Data Loss due to Hardware Failure AD	55/10	25/10	45/14
Data Loss due to Hardware Failure MOD	50/10	25/10	50/25

Table A.12.: Risk-related AVC and RUC Effectiveness (Asset Value Pres. / Security Status)

Risk	AVS A	AVS B	AVS C	Weekly Upd.	Daily Upd.
Malware Infection DBS	35/75	40/80	45/85	65/65	85/85
Malware Infection AS	35/75	45/90	40/85	65/65	85/85
Malware Infection WS	35/75	50/85	45/95	60/60	85/85
Unwanted Tampering with Software SS	25/55	30/65	35/70	70/70	75/75
Unwanted Tampering with Software CS	25/55	30/70	25/75	70/70	75/75
Unwanted Tampering with Software DMS	40/80	50/90	50/90	70/70	90/90
Loss of Data Confidentiality MW-RD	65/15	75/25	80/35	65/15	85/30
Loss of Data Confidentiality MW-RDB	65/15	80/25	80/25	70/20	90/35
Loss of Data Confidentiality MW-AD	65/15	75/25	80/35	65/15	85/30
Loss of Data Confidentiality MW-MOD	55/10	65/20	75/25	60/15	85/30

Table A.13.: Risk-related FWC Effectiveness (Asset Value Pres. / Security Status)

Risk	Firewall A	Firewall B	Firewall C	Firewall D	Firewall E
Intrusion into System DBS	15/65	20/75	25/75	20/80	25/95
Intrusion into System AS	15/65	25/70	30/80	25/85	20/85
Network Eavesdropping	0/25	0/75	0/80	0/85	0/90
Ext. Data Theft / Manipulation RD	75/25	80/30	70/25	90/35	80/30
Ext. Data Theft / Manipulation RDB	70/20	85/35	90/35	95/35	80/30
Ext. Data Theft / Manipulation AD	75/25	80/30	70/25	90/37	80/30
Ext. Data Theft / Manipulation MOD	75/25	80/30	70/25	90/38	80/30

Table A.14.: Risk-related ACC Effectiveness (Asset Value Pres. / Security Status)

Risk	User Rights Restriction	Enhanced Password Policy
Impersonation	0/75	0/80
Ext. Data Theft / Manipulation RD	45/45	60/60
Ext. Data Theft / Manipulation RDB	45/45	60/60
Ext. Data Theft / Manipulation AD	45/45	60/60
Ext. Data Theft / Manipulation MOD	45/45	60/60
Internal Data Manipulation RD	70/70	85/85
Internal Data Manipulation RDB	70/70	85/85
Internal Data Manipulation AD	70/70	85/85
Internal Data Manipulation MOD	70/70	85/85
Unwanted Money Transfers	80/80	80/80

Table A.15.: Risk-related ECC Effectiveness (Asset Value Pres. / Security Status)

Risk	SK Encryption	PK Encryption
Network Eavesdropping	0/90	0/95
Eavesdropping of Mails	0/90	0/95
Eavesdropping of Money Transfers	0/90	0/95
Unwanted Money Transfers	85/85	95/95

Table A.16.: Risk-related PPC Effectiveness (Asset Value Pres. / Security Status)

Risk	Physical Locks	Surveillance Syst.	Security Guards
Sabotage by internal Threat Agent DBS	50/10	85/15	95/35
Sabotage by internal Threat Agent AS	50/10	85/15	95/35
Sabotage by internal Threat Agent WS	35/10	80/10	90/30
Sabotage by internal Threat Agent NI	45/10	85/10	95/35
Data Loss due to Hardware Sabotage RD	45/10	85/10	95/35
Data Loss due to Hardware Sabotage RDB	50/10	85/15	95/35
Data Loss due to Hardware Sabotage AD	50/10	85/15	95/35
Data Loss due to Hardware Sabotage MOD	50/10	85/15	95/35

Table A.17.: Risk-related ETC Effectiveness (Asset Value Pres. / Security Status)

Risk	Basic Training	Ext. Training
Data Entry Error SS	0/25	0/30
Data Entry Error CS	0/25	0/30
Data Entry Error DMS	0/25	0/30
Error Overlooking SS	0/25	0/30
Error Overlooking CS	0/25	0/30
Error Overlooking DMS	0/25	0/30
Unwanted Tampering with Software SS	25/70	30/85
Unwanted Tampering with Software CS	25/70	30/85
Unwanted Tampering with Software DMS	30/75	45/90
Offline Industrial Espionage RD	60/60	85/85
Offline Industrial Espionage RDB	60/60	85/85
Offline Industrial Espionage AD	60/60	85/85

Table A.18.: Risk-related BSC Effectiveness (Asset Value Pres. / Security Status)

Risk	Backup A	Backup B	Backup C	Backup D
Data Loss due to Power Failure RD	70/70	85/85	90/90	95/95
Data Loss due to Power Failure RDB	70/70	85/85	90/90	95/95
Data Loss due to Power Failure AD	70/70	85/85	90/90	95/95
Data Loss due to Power Failure MOD	70/70	85/85	90/90	95/95

Table A.19.: Risk-related SLC Effectiveness (Asset Value Pres. / Security Status)

Risk	Fault Logging	Full Logging
Inconsistent Money Order Data	95/95	100/100
E-Mail Problems	80/80	85/85
Repudiation of Money Transfers	95/95	100/100

A.3. AHP Example Data

Table A.20.: Asset Value Preservation Prioritization (Benefit)

Asset Value Preservation	Asset Value	Risk Reduction	Number of P. Assets	Priority
Asset Value	1	3	2	0,249
Risk Reduction	1/3	1	3	0,594
Number of P. Assets	1/2	1/3	1	0,157

Table A.21.: Process Benefit Prioritization (Benefit)

Process Benefit	Asset Importance	Protection Effectiveness	Priority
Asset Importance	1	2	0,667
Portection Effectiveness	1/2	1	0,333

Table A.22.: Benefit Prioritization

Benefit	Asset Value Preservation	Security Status	Process Benefit	User Acceptance	Priority
Asset Value Preservation	1	3	2	3	0,441
Security Status	1/3	1	3	2	0,152
Process Benefit	1/2	1/3	1	2	0,290
User Acceptance	1/3	1/2	1/2	1	0,117

Table A.23.: Productivity Loss Prioritization (Cost)

Productivity Loss	**Asset Impact**	**Safeguard Impediment**	**Priority**
Asset Impact	1	2	0,667
Safeguard Impediment	1/2	1	0,333

Table A.24.: Cost Prioritization

Cost	**Setup Cost**	**Running Cost**	**Maint. Time**	**Prod. Loss**	**Priority**
Setup Cost	1	2	3	2	0,219
Running Cost	1/2	1	2	2	0,273
Maintenance Time	1/3	1/2	1	2	0,125
Productivity Loss	1/2	1/2	1/2	1	0,383

Table A.25.: Alternative Ratings (Benefit)

Alternative	**AV(AVP)**	**RR(AVP)**	**NA(AVP)**	**SS**	**AI**	**PE**	**UA**
Backup A	0,232	0,343	0,382	0,112	1,000	0,382	0,627
Backup B	0,232	0,343	0,382	0,112	1,000	0,627	0,382
Backup C	0,232	0,589	0,382	0,112	1,000	0,627	0,382
Backup D	0,232	0,589	0,382	0,112	1,000	1,000	0,232
Regular Maint.	1,000	0,199	0,627	0,112	0,627	0,148	0,382
Basic Fallback	1,000	0,116	0,627	0,112	0,627	0,148	0,382
Full Fallback	1,000	0,199	0,627	0,112	0,627	0,232	0,382
Weekly Upd.	1,000	1,000	1,000	1,000	0,382	0,148	0,627
Daily Upd.	1,000	1,000	1,000	1,000	0,382	0,232	0,382
Scanner A	1,000	1,000	1,000	1,000	0,382	0,232	0,627
Scanner B	1,000	1,000	1,000	1,000	0,382	0,382	0,627
Scanner C	1,000	1,000	1,000	1,000	0,382	0,382	0,627
SK Encr.	0,627	0,199	0,232	0,195	0,232	0,382	0,382
PK Encr.	0,627	0,199	0,232	0,195	0,232	0,627	0,382
Firewall A	1,000	0,199	0,627	0,112	0,627	0,382	0,382
Firewall B	1,000	0,343	0,627	0,195	0,627	0,382	0,382
Firewall C	1,000	0,343	0,627	0,195	0,627	0,627	0,232
Firewall D	1,000	0,343	0,627	0,195	0,627	0,232	0,627
Firewall E	1,000	0,343	0,627	0,195	0,627	0,382	0,232
Fault Logging	0,382	0,589	0,232	0,335	0,232	0,148	0,382
Full Logging	0,382	1,000	0,232	0,335	0,232	0,232	0,232
Port. Fire Ext.	0,627	0,118	0,627	0,112	0,627	0,382	0,382
Fixed Fire Ext.	0,627	0,118	0,627	0,112	0,627	0,627	0,382
Physical Locks	1,000	0,118	0,627	0,112	0,627	0,232	0,232
Surv. System	1,000	0,118	0,627	0,112	0,627	0,382	0,148
Sec. Guards	1,000	0,118	0,627	0,112	0,627	0,382	0,148
Basic Training	0,382	0,199	0,382	0,335	0,627	0,148	0,148
Ext. Training	0,382	0,343	0,382	0,335	0,627	0,232	0,148
User Rights. Restr.	1,000	0,343	0,382	0,195	0,382	0,382	0,148
Enh. Password Pol.	1,000	0,343	0,382	0,195	0,382	0,382	0,148

Table A.26.: Alternative Ratings (Cost)

Alternative	**SC**	**RC**	**MTE**	**AI(PL)**	**SI(PL)**
Backup A	0,148	0,232	0,382	1,000	0,148
Backup B	0,382	0,382	0,627	1,000	0,148
Backup C	0,382	0,382	0,627	1,000	0,148
Backup D	0,382	0,382	1,000	1,000	0,148
Regular Maint.	0,148	0,382	0,382	0,627	0,627
Basic Fallback	0,382	0,382	0,382	0,627	0,627
Full Fallback	1,000	0,382	0,382	0,627	0,627
Weekly Upd.	0,148	0,232	0,148	0,382	0,328
Daily Upd.	0,148	0,382	0,232	0,382	0,627
Scanner A	0,148	0,148	0,148	0,382	0,627
Scanner B	0,232	0,232	0,148	0,382	1,000
Scanner C	0,232	0,232	0,148	0,382	1,000
SK Encr.	0,232	0,232	0,232	0,232	1,000
PK Encr.	0,232	0,382	0,232	0,232	1,000
Firewall A	0,148	0,148	0,148	0,627	0,627
Firewall B	0,232	0,232	0,148	0,627	0,627
Firewall C	0,232	0,232	0,148	0,627	0,627
Firewall D	0,232	0,232	0,148	0,627	0,627
Firewall E	0,232	0,232	0,232	0,627	1,000
Fault Logging	0,148	0,232	0,382	0,232	0,382
Full Logging	0,148	0,232	0,627	0,232	0,382
Port. Fire Ext.	0,232	0,232	0,148	0,627	0,148
Fixed Fire Ext.	1,000	0,382	0,232	0,627	0,148
Physical Locks	0,232	0,232	0,148	0,627	0,382
Surv. System	0,627	0,382	0,627	0,627	0,627
Sec. Guards	0,232	0,627	0,627	0,627	0,627
Basic Training	0,148	0,627	0,232	0,627	0,627
Ext. Training	0,148	1,000	0,382	0,627	1,000
User Rights. Restr.	0,232	0,627	0,232	0,382	1,000
Enh. Password Pol.	0,232	0,382	0,232	0,382	0,627

A.4. POSeM Example Data

Table A.27.: Consistency Checks

ID	Triplet	Conf.	Int.	Avail.	Acc.
p1	Preparer	high	med	med	med
a1	Register Request	high	med	high	med
o1	Request Data	high	high	med	med
			x	x	
p1	Preparer	high	med	med	med
a2	Check Request for Eligibility	high	high	med	med
o3	Applicant's Insurance Status	high	high	med	med
			x		
p1	Preparer	high	med	med	med
a2	Check Request for Eligibility	high	high	med	med
o1	Request Data	high	high	med	med
			x		
p4	E-Mail System	med	med	low	high
a3	Return Request to Applicant	med	med	med	med
o5	Request Return Mail	med	high	low	med
			x	x	
p1	Preparer	high	med	med	med
a4	Scan Request	med	high	med	med
o1	Request Data	high	high	med	med
		x	x		
p1	Preparer	high	med	med	med
a5	Check Request for Uniqueness	high	high	med	med
o1	Request Data	high	high	med	med
			x		
p1	Preparer	high	med	med	med
a5	Check Request for Uniqueness	high	high	med	med
o2	Request Data (DB)	high	high	med	med
			x		
p2	Assistant	med	med	med	med
a6	Process Request	med	med	med	med
o1	Request Data	high	high	med	med
		x	x		
p2	Assistant Worker	med	med	med	med
a7	Mark for Approval Support	med	med	med	med
o1	Request Data	high	high	med	med
		x	x		
p3	Supervisor	very high	high	med	high
a8	Open Marked Documents (SV)	high	high	med	high
o1	Request Data	high	high	med	med
p2	Assistant	med	med	med	med
a9	Edit Request	med	med	med	med
o1	Request Data	high	high	med	med
		x	x		

Table A.28.: Consistency Checks - Cont.

ID	Triplet	Conf.	Int.	Avail.	Acc.
p2 a10 o1	Assistant Check Correctness Support Request Data	med high high	med high high	med med med	med med med
		x	x		
p4 a11 o5	E-Mail System Inform Applicant Request Return Mail	med med med	med med high	low med low	high med med
			x	x	
p5 a12 o4	External Web Service Send Money Order Money Order Data	very high very high very high	very high very high very high	med med med	high high high

Table A.29.: Consistent Clearance Levels for Actors

ID	Participant	Type (opt.)	Conf.	Int.	Avail.	Acc.
p1	Preparer	Human	high	med->high	med-high	med
p2	Assistant	Human	med->high	med->high	med	med
p3	Supervisor	Human	very high	very high	med	high
p4	E-Mail System	System	med	med->high	low->med	high
p5	Ext. Web Service	System	very high	very high	med	high

Table A.30.: Consistent Security Levels for Activities

ID	Activity	Type (opt.)	Conf.	Int.	Avail.	Acc.
a1	Register Request		high	med->high	high	med
a2	Check Request for Eligibility		high	high	med	med
a3	Return Request to Applicant	Transfer	med	med->high	med	med
a4	Scan Request		med->high	high	med	med
a5	Check Request for Uniqueness	Storage	high	high	med	med
a6	Process Request		med->high	med->high	med	med
a7	Mark for Approval		med->high	med->high	med	med
a8	Open Marked Documents (SV)		high	high	med	high
a9	Edit Request		med->high	med	med	med
a10	Check Correctness		high	high	med	med
a11	Inform Applicant	Transfer	med	med->high	med	med
a12	Send Money Order	Transfer	very high	very high	med	high

Table A.31.: Consistent Security Levels for Artifacts (Data)

ID	Data	Type (opt.)	Conf.	Int.	Avail.	Acc.
o1	Request Data	Data	high	high	med	med
o2	Request Data (DB)	Data	high	high	med	med
o3	Applicant's Insurance Status	Data	high	high	med	med
o4	Money Order Data	Data	very high	very high	med	high
o5	Request Return Mail	Data	med	high	low	med

Table A.32.: Security Controls List

ID	Module	Measure	Obs.	Dep.
s1	Standards, Policies, Guidelines	Integrated S Policy Documentation		
s2	Standards, Policies, Guidelines	Major Policy Review		s1
s3	Standards, Policies, Guidelines	Periodic Management IS Forum		
t1a	Training, Awareness, Pers. Rel. M.	Employee Training (basic)		
t1b	Training, Awareness, Pers. Rel. M.	Employee Training (ext.)	t1a	
t1c	Training, Awareness, Pers. Rel. M.	Employee Training (full)	t1a,t1b	
e1a	Physical, Environmental Meas.	Fire Extinguisher (port)		
e1b	Physical, Environmental Meas.	Fire Extinguisher (fixed)	e1a	
e2	Physical, Environmental Meas.	Physical Security Perimeter		
e3	Physical, Environmental Meas.	Physical Access Control (card + PIN)		
e4	Physical, Environmental Meas.	Physical Locks (Equipment)		
e5	Physical, Environmental Meas.	Backup Generators		
e6	Physical, Environmental Meas.	Cable Security (Shielding)		
e7	Physical, Environmental Meas.	Surveillance System		
e8	Physical, Environmental Meas.	Security Guards		e7
au1a	Checks, Audit Procedures	Event Logging (fault)		
au1b	Checks, Audit Procedures	Event Logging (full)	au1a	
o1	Operations	Dual Input (Validation)		
o2a	Operations	Secure Storage Media Disposal		
o2b	Operations	Storage Destruction	o2a	
o3a	Operations	Backups (min)		
o3b	Operations	Backups (raid)	o3a	
o3c	Operations	Backups (tape)	o3a,o3b	
o3d	Operations	Backups (double)	o3a,o3b,o3c	
o4	Operations	Hardware Maintenance		
o5a	Operations	Fallback Equipment (basic)		
o5b	Operations	Fallback Equipment (full)		
i1a	IT Specific: Ident, Authent.	Basic A + A (User ID and Password)		
i1b	IT Specific: Ident, Authent.	Ext. A + A (Smart Card Token)		
a1a	IT Specific: Access Control	General AC		
a1b	IT Specific: Access Control	Strict User Rights Restriction	a1a	
a2	IT Specific: Access Control	Enh. Password Policy		
a3	IT Specific: Access Control	Periodical Review of Access Rights		a1
v1a	IT Specific: Prot. against Mal. Code	Virus Scanner A		
v1b	IT Specific: Prot. against Mal. Code	Virus Scanner B		
v1c	IT Specific: Prot. against Mal. Code	Virus Scanner C		
v2	IT Specific: Prot. against Mal. Code	Check Incoming Mail Att.		v1
v3a	IT Specific: Prot. against Mal. Code	Weekly Virus Updates		
v3b	IT Specific: Prot. against Mal. Code	Daily Virus Updates	v3a	
n1	IT Specific: Network Management	Intrusion Detection		
n2	IT Specific: Network Management	Penetration Testing		
n3a	IT Specific: Network Management	Firewall A		
n3b	IT Specific: Network Management	Firewall B	n3a	
n3c	IT Specific: Network Management	Firewall C	n3a	
n3d	IT Specific: Network Management	Firewall D	n3a	
n3e	IT Specific: Network Management	Firewall E	n3a	
c1	IT Specific: Cryptography	Encryption A (SK)		c4
c2	IT Specific: Cryptography	Encryption B (PK)	c1	c4
c3	IT Specific: Cryptography	Digital Sign. (Smart Card)		c4
c4	IT Specific: Cryptography	Secure Key Generation		

Table A.33.: Safeguard Derivation Rules (RB2)

		Conf.			**Int.**			**Avail.**			**Acc.**		
ID	**Control**	**P**	**O**	**A**	**P**	**O**	**A**	**P**	**O**	**A**	**P**	**O**	**A**
s1	Integrated S Policy Doc.	2	-	-	2	-	-	2	-	-	2	-	-
s2	Major Policy Review	3H	-	-	3H	-	-	3H	-	-	3H	-	-
s3	Periodic Management IS Forum	4H	-	-	4H	-	-	4H	-	-	4H	-	-
t1a	Empl. Training (basic)	2H	-	-	2H	-	-	2H	-	-	2H	-	-
t1b	Empl. Training (ext.)	3H	-	-	3H	-	-	3H	-	-	3H	-	-
t1c	Empl. Training (full)	4H	-	-	4H	-	-	4H	-	-	4H	-	-
e1a	Fire Extinguisher (port)	-	-	-	2	-	-	2	-	-	-	-	-
e1b	Fire Extinguisher (fixed)	-	-	-	3	-	-	3	-	-	-	-	-
e2	Physical Security Perimeter	3	-	-	3	-	-	3	-	-	3	-	-
e3	Physical Access Control	4H	4	-	4H	4	-	4H	-	4	4H	4	-
e4	Physical Locks (Equipment)	2S	2	2	2S	2	2	2S	2	2	2S	2	2
e5	Backup Generators	-	-	-	-	-	-	4S	4D	-	-	-	-
e6	Cable Security (Shielding)	3S	3D	3T	3S	3D	3T	3S	3D	3T	3S	3D	3T
e7	Surveillance System	3H	-	3	3H	-	3	3H	-	3	3H	-	3
e8	Security Guards	4H	-	4	4H	-	4	4H	-	4	4H	-	4
au1a	Event Logging (fault)	-	-	-	2S	2D	2	-	-	-	2S	2D	2
au1b	Event Logging (full)	-	-	-	3S	3D	3	-	-	-	3S	3D	3
o1	Dual Input (Validation)	-	-	-	3H	3D	3	3H	3D	3	-	-	-
o2a	Secure Storage Media Disposal	2S	2D	2	-	-	-	-	-	-	-	-	-
o2b	Storage Destruction	4S	4	4S	-	-	-	-	-	-	4S	4	4S
o3a	Backups (min)	-	-	-	-	-	-	1S	1	1S	-	-	-
o3b	Backups (raid)	-	-	-	-	-	-	2S	2	2S	-	-	-
o3c	Backups (tape)	-	-	-	-	-	-	3S	3	3S	-	-	-
o3d	Backups (double backup)	-	-	-	-	-	-	4S	4	4S	-	-	-
o4	Hardware Maintenance	1S	1D	1	1S	1D	1	1S	1D	1	1S	1D	1
o5a	Fallback Equipment (basic)	-	-	-	-	-	-	2S	2D	2	-	-	-
o5b	Fallback Equipment (full)	-	-	-	-	-	-	4S	4D	4	-	-	-
i1a	Basic A + A	2	2D	2	2	2D	2	2	2D	2	2	2D	2
i1b	Ext. A + A (Smart Card Token)	4	4D	4	4	4D	4	4	4D	4	4	4D	4
a1a	General AC	2H	2D	2	2H	2D	2	2H	2D	2	2H	2D	2
a1b	Strict User Rights Restriction	3H	3D	3	3H	3D	3	3H	3D	3	3H	3D	3
a2	Enh. Password Policy	3	3D	3	3	3D	3	3	3D	3	3	3D	3
a3	Periodical Review of Access Rights	4	4D	4	4	4D	4	4	4D	4	4	4D	4
v1a	Virus Scanner A	1	1	1	1	1	1	1	1	1	1	1	1
v1b	Virus Scanner B	2	2	2	2	2	2	2	2	2	2	2	2
v1c	Virus Scanner C	2	2	2	2	2	2	2	2	2	2	2	2
v2	Check Incoming Mail Att.	1	1D	1T	1	1D	1T	1	1D	1T	1	1D	1T
v3a	Weekly Virus Updates	1	1	1	1	1	1	1	1	1	1	1	1
v3b	Daily Virus Updates	2	2	2	2	2	2	2	2	2	2	2	2
n1	Intrusion Detection	3	3	3T	3	3	3T	3	3	3T	3	3	3T
n2	Penetration Testing	4	4	4T	4	4	4T	4	4	4T	4	4	4T
n3a	Firewall A	1	1	1	1	1	1	1	1	1	1	1	1
n3b	Firewall B	2	2	2	2	2	2	2	2	2	2	2	2
n3c	Firewall C	2	2	2	2	2	2	2	2	2	2	2	2
n3d	Firewall D	2	2	2	2	2	2	2	2	2	2	2	2
n3e	Firewall E	2	2	2	2	2	2	2	2	2	2	2	2
c1	Encryption A (SK)	3	3D	3	3	3D	3	-	-	-	3	3D	3
c2	Encryption B (PK)	4	4D	4	4	4D	4	-	-	-	4	4D	4
c3	Digital Sign. (Smart Card)	3H	-	-	4H	-	-	-	-	-	4H	-	-
c4	Secure Key Generation	2	2D	2	2	2D	2	-	-	-	2	2D	2

Table A.34.: Module Applicability

Component	**S**	**T**	**E**	**Au**	**O**	**I**	**A**	**V**	**N**	**C**
Preparer	x	x			x	x	x	x		x
Assistant	x	x			x	x	x	x		x
Supervisor	x	x				x	x	x		x
E-Mail System	x		x	x	x	x	x			x
External Webservice	x			x		x	x			x
Request Data			x	x	x	x	x	x		
Request Data (DB)			x	x	x	x	x	x		x
App. Insurance Status			x	x	x	x	x	x		x
Money Order Data				x		x	x	x		x
Return Mail			x	x	x	x	x	x		x
Register Request				x	x	x	x	x		x
check Eligibility					x	x	x	x	x	
Return Request					x			x		x
Scan Request					x	x	x	x	x	
Check Uniqueness					x	x	x	x	x	
Process Request					x	x	x	x	x	
Mark for Approval					x				x	
Open Docs (SV)					x	x	x	x	x	x
Edit Request					x	x	x	x	x	
check Correctness					x	x	x	x	x	
Inform Applicant				x	x			x		x
Send Money Order				x		x	x		x	x

Bibliography

[AdBD$^+$02] J. O. Aagedal, F. den Braber, T. Dimitrakos, B. A. Gran, D. Raptis, and K.l Stolen. Model-based risk assessment to improve enterprise security. In *Proc. Enterprise Distributed Object Communication (EDOC'2002)*, pages 51–62. IEEE Computer Society, 2002.

[ADSW03] C. Alberts, A. Dorofee, J. Stevens, and C. Woody. Introduction to the octave approach. Technical report, Carnegie Mellon Software Engineering Institute, August 2003.

[AJ95] M. D. Abrams and S. Jajodia. *Information Security: An Integrated Collection of Essays*. IEEE Computer Society Press, 1995.

[ALRL04] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 01(1):11–33, 2004.

[And03] J. M. Andersen. Why we need a new definition of information security. *Computers and Security*, 22(4):308–313, May 2003.

[Bal96] H. Balzert. *Lehrbuch der Software-Technik: Software-Entwicklung*. Spektrum Akademischer Verlag, 1996.

[BBSK06] A. Baldwin, Y. Beres, S. Shiu, and P. Kearney. A model-based approach to trust, security and assurance. *BT Technology Journal*, 24(4):53–68, 2006.

[BDL06] D. Basin, J. Doser, and T. Lodderstedt. Model driven security: From uml models to access control infrastructures. *ACM Transactions on Software Engineering and Methodology*, 15(1):39–91, January 2006.

[BF02] S. A. Butler and P. Fischbeck. Multi-attribute risk assessment. In *Proceedings of SREIS '02*, Raleigh, NC, 2002.

[BG83] V. Belton and T. Gear. On a short-coming of saaty's method of analytic hierarchies. *Omega*, 11(3):228–230, 1983.

[BGL05] Lawrence D. Bodin, Lawrence A. Gordon, and Martin P. Loeb. Evaluating information security investments using the analytic hierarchy process. *Commun. ACM*, 48(2):78–83, 2005.

[Bis03] M. Bishop. What is computer security? *IEEE Security & Privacy Magazine*, 1(1):67–69, 2003.

[BMG01] B. Blakley, E. McDermott, and D. Geer. Information security is information risk management. In *NSPW '01: Proceedings of the 2001 workshop on New security paradigms*, pages 97–104, New York, NY, USA, 2001. ACM Press.

[BOC04] BOC. *Adonis Version 3.81*, 2004.

[Bor04] W. G. Bornman. *Information Security Risk Managemet: A Hollistic Framework*. Phd thesis, Faculty of Economic and Managemet Sciences, Rand Africaans University, October 2004.

[Bri00] A. Briney. Security focused - the 2000 information security industry survey. *Information Security Magazine*, pages 40–68, 2000.

[BSI99] BSI. Bs7799 - code of practice for information security management. British Standards Institute, 1999.

[But02] Shawn A. Butler. Security attribute evaluation method: a cost-benefit approach. In *ICSE '02: Proceedings of the 24th International Conference on Software Engineering*, pages 232–240, New York, NY, USA, 2002. ACM Press.

[But03] S. A. Butler. *Security Attribute Evaluation Method*. Phd thesis, School of Computer Science, Carnegie Mellon University, March 2003.

[Buz99] K. Buzzard. Computer security - what should you spend your money on? *Computers and Security*, 18:322–334, 1999.

[BvUzMR99] J. Becker, C. von Uthmann, M. zur Mühlen, and M. Rosemann. Identifying the workflow potential of business processes. In *Proceedings of* *the 32nd Hawaii International Conference on System Sciences*, volume 5. IEEE, 1999.

[BW95] P. Barthelmess and J. Wainer. Workflow systems: a few definitions and a few suggestions. In *COCS '95: Proceedings of conference on Organizational computing systems*, pages 138–147, New York, NY, USA, 1995. ACM Press.

[CBS04] J. Cardoso, R. P. Bostrom, and A. Sheth. Workflow management systems vs. erp systems: Differences, commonalities, and applications. *Information Technology and Management Journal*, 5(3-4):319–338, 2004.

[CER07] CERT. Octave. Online at http://www.cert.org/octave/index.html, September 2007.

[CFBZC02] T. J. Crowe, P. M. Fong, T. A. Bauman, and J. L. Zayas-Castro. Quantitative risk level estimation of business process reengineering efforts. *Business Process Management Journal*, 8(5):490–511, 2002.

[Che76] P. P. Chen. The entity-relationship model: Towards a unified view for data. *ACM Transactions on Database-Systems*, 1(1):9–36, 1976.

[CKL$^+$05] Y.-J. Chung, I.-J. Kim, N.-H. Lee, T. Lee, and H. P. In. Security risk vector for quantitative asset assessment. In *Computational Science and Its Applications - ICCSA 2005*. Springer, 2005.

[CKO92] B. Curtis, M. I. Kellner, and J. Over. Process modeling. *Communications of the ACM*, 35(9):75–90, 1992.

[CLS89] W. Caelli, D. Longley, and M. Shain. *Information Security for Managers.* Stockton Press, 1989.

[Col04] J. Coleman. Assessing information security risk in healthcare organizations of different scale. In *Proceedings of the 18th International Congress and Exhibiiton, CARS 2004 - Computer Assisted Radiology and Surgery*, pages 125–130. Elsevier, 2004.

[Com04] ComputerEconomics. The cost impact of major virus attacks since 1995. Online at http://www.computereconomics.com, February 2004.

[Cou77] R. Courtney. Security risk analysis in electronic data processing. In *AFIPS Conference Proceedings NCC*. AFIPS Press, 1977.

[cra05] The logic behind cramm's assessment of measures of risk and determination of appropriate countermeasures. Technical report, Insight Consulting, October 2005.

[DRRS02] T. Dimitrakos, D. Raptis, B. Ritchie, and K. Stolen. Model based security risk analysis for web applications. In *Proc. Euroweb 2002*. British Computer Society, 2002.

[Dye90] J. S. Dyer. Remarks on the analytic hierarchy process. *Management Science*, 36(3):249–258, 1990.

[EHLB95] D. J. Elzinga, T. Horak, C.-Y. Lee, and C. Bruner. Business process management: Survey and methodology. In *IEEE Transactions on Engineering Management*, volume 42, pages 119–128. IEEE, May 1995.

[eni06] Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools. Technical report, European Network and Information Security Agency (ENISA), June 2006.

[Fin98] T. Finne. A conceptual framework for information security management. *Computers & Security*, 17:303–307, 1998.

[Fin00] T. Finne. Information systems risk management: Key concepts and business processes. *Computers and Security*, 19:234–242, 2000.

[fip79] Fips Publication (65), 1979.

[FKG+02] Rune Fredriksen, Monica Kristiansen, Bjorn Axel Gran, Ketil Stolen, Tom Arthur Opperud, and Theodosis Dimitrakos. The coras framework for a model-based risk management process. In *SAFECOMP '02: Proceedings of the 21st International Conference on Computer Safety, Reliability and Security*, pages 94–105, London, UK, 2002. Springer-Verlag.

[FNES03] F. Farahmand, S. B. Navathe, P. H. Enslow, and G. P. Sharp. Managing vulnerabilities of information systems to security incidents. In *ICEC '03: Proceedings of the 5th international conference on Electronic commerce*, pages 348–354, New York, NY, USA, 2003. ACM Press.

[FS93] O. K. Ferstl and E. J. Sinz. Business process modelling. *Wirtschaftsinformatik*, 35(6):589–592, 1993.

[Gal04] L. Galway. Quantiative risk analysis for project management - a critical review. White Paper, February 2004.

[GC04] D. Gotterbarn and T. Clear. Using sodis as a risk analysis process: A teaching perspective. In *Proceedings of the Sixth Australasian Computing Education Conference (ACE2004)*, Dunedin, New Zealand, June 2004.

[GK95] H. A. Gartner and P. Konrad. Nutzung von Methoden und Instrumenten - Details zur KES Sicherheitsstudie 1994. *KES - Zeitschrift für Kommunikations- und EDV Sicherheit*, 2, 1995.

[GL02] L. A. Gordon and M. P. Loeb. The economics of information security investment. *ACM Transactions on Information Systems Security*, 5(4):438–457, 2002.

[GLWH03] B. C. Guan, C. C. Lo, P. Wang, and J. S. Hwang. Evaluation of information security related risks of an organization: the application of the multicriteria decision-making method. In *Proceedings of the 37th Annual 2003 Internation Carnahan Conference on Security Technology*, pages 168–175, October 2003.

[Gru00] P. Gruenbacher. Collaborative requirements negotiation with easywinwin. In *Proceedings of the 11th International Workshop on Database and Expert Systems Applications DEXA '00*, page 954, Washington, DC, USA, 2000. IEEE Computer Society.

[Gua87] S. B. Guano. Principles and procedure of the lram approach to information systems risk analysis and management. *Computers and Security*, 6:493–504, 1987.

[Ham96] M. Hammer. *Beyond Reengineering - How the process-centered organization is changing our work and our livesw*, chapter The Triumph of Process, pages 3–17. HarperCollins, 1996.

[Ham02] C. R. Hamilton. Risk management & security. White Paper, RiskWatch, 2002.

[Han03] HandySoft Global Corporation, Vienna, USA. *Business Process Management and its Value to the Enterprise*, white paper edition, October 2003.

[Her99] G. Herrmann. Security and integrity requirements of business processes - analysis and approach to support their realisation. In *Consortium on Advanced Information Systems Engineering*, pages 36–47, 1999.

[HH06] Peter Herrmann and Gaby Herrmann. Security requirement analysis of business processes. *Electronic Commerce Research*, 6(3-4):305–335, 2006.

[HLR00] K. K. S. Ho, E. Leroi, and W.J. Roberds. Quantitative risk assessment applications, myths and future direction. In *Proceedings of the International Conference on Geotechnical and Geological Engineering (GeoEng 2000),*, pages 269–312, Melbourne, 2000.

[HM99] C. Hastedt-Marckwardt. Workflow management systeme: Ein beitrag der it zur geschäftsprozeß-orientierung & -optimierung - grundlagen, standards und trends. In *Informatik Spektrum*, volume 22, pages 99–109. Springer, 1999.

[Ho07] W. Ho. Integrated analytic hierarchy process and its applications - a literature review. *European Journal of Operational Research*, 2007.

[Hol90] R. D. Holder. Some comments on the analytic hierarchy process. *Journal of the Operational Research Society*, 41(11):1073–1076, 1990.

[HP98] G. Herrmann and G. Pernul. Viewing business process security from different perspectives. In *Proceedings of 11th International Bled Electronic Commerce Conference 'Electronic Commerce in the Information Society'*, pages 89–103, 1998.

[HWHL03] C. H. Han, R. H. Westen, A. Hodgson, and K. H. Lee. The complementary use of idef and uml modelling approaches. *Computers in Industry*, 50:35–56, 2003.

[IBM84] IBM. Ibm data security support programs, 1984.

[IDS04] IDS Scheer. *ARIS 6 - Collaborative Suite - ARIS Method*, July 2004.

[Ins07] InsightConsulting. Cramm. Online at http://www.cramm.com, Access in May 2007.

[IST07] IST. The coras project. Online at http://coras.sourceforge.net, Access in May 2007.

[Jas04] A. Jaszkiewicz. Evaluation of multiple objective metaheuristics. In *Metaheuristics for Multiobjective Optimisation*. Springer, 2004.

[JEJ94] I. Jacobson, M. Ericsson, and A. Jacobson. *The object advantage: business process reengineering with object technology.* ACM Press/Addison-Wesley Publishing Co., New York, NY, USA, 1994.

[JEJ95] I. Jacobson, M. Ericson, and A. Jacobson. *The Object Advantage - Business Process Reengineering with Object Technology.* Addison-Wesley, 1995.

[JMV$^+$07] A. K. Jallow, B. Majeed, K. Vergidis, A. Tiwari, and R. Roy. Operational risk analysis in business processes. *BT Technology Journal*, 25(1):168–177, January 2007.

[Joh04] S. Johnston. Rational uml profile for business modeling. Technical report, IBM Rational, 2004.

[Jon07] A. Jones. A framework for the management of information security risks. *BT Technology*, 25(1):30–36, January 2007.

[Jür02] J. Jürjens. Umlsec: Extending uml for secure systems development. In *UML 2002*. Springer, 2002.

[Kat07] S. Katzke. Security metrics. Online at `http://www.cs.msstate.edu/~ia/IA_PAPERS/Katzke.pdf`, Access in May 2007.

[KDK00] S. A. Kokolakis, A. J. Demopoulos, and E. A. Kiountouzis. The use of business process modeling in information systems security analysis and design. *Information Management & Computer Security*, 8(3):107–116, 2000.

[Ked00] P. Kedrosky. Hackers prey on our insecurities. The Wall Street Journal, February 2000.

[Kob99] C. Kobryn. Uml 2001: a standardization odyssey. *Commununications of the ACM*, 42(10):29–37, 1999.

[Lan01] C.E. Landwehr. Computer security. *International Journal of Information Security*, 1(1):3–13, 2001.

[LD98] R. G. Lee and B. G. Dale. Business process management: a review and evaluation. *Business Process Re-engineering & Management Journal*, 4(3):214–225, 1998.

[LDL03] A. Lindsay, D. Downs, and K. Lunn. Business processes - attempts to find a definition. *Information and Software Technology*, 45(1):1015–1019, 2003.

[LHSS03] M. S. Lund, I. Hogganvik, F. Seehusen, and K.l Stolen. Uml profile for security assessment. Technical report, SINTEF Information and Communication Technology, November 2003.

[Li07] Y. Li. *An Intelligent, Knowledge-based Multiple Criteria Decision Making Advisor for Systems Design*. Phd thesis, School of Aerospace Engineering, Georgia Institute of Technology, May 2007.

[LK05] B. List and B. Korherr. A uml 2 profile for business process modelling. In *Proceedings of the 1st International Workshop on Best Practices of UML (BP-UML 2005) at the 24th International Conference on Conceptual Modeling (ER2005)*, 2005.

[LK06] B. List and B. Korherr. Extending the uml 2 activity diagram with business process goals and performance measures and the mapping to bpel. In *Proceedings of the 2nd International Workshop on Best Practices of UML (BP-UML 2006) at the 25th International Conference on Conceptual Modeling (ER 2006)*, 2006.

[LPS05] S. Lusk, S. Paley, and A. Spanyi. The evolution of business process management as a professional discipline. Technical report, ABPMP, June 2005.

[LV04] A. Lenstra and T. Voss. Information security risk assessment, aggregation and mitigation. In *Information Security and Privacy*, volume 3108 of *Lecture Notes in Comuter Science*, pages 391–401. Springer Berlin, June 2004.

[MC05] R. Mock and M. Corvo. Risk analysis of information systems by event process chains. *International Journal of Critical Infrastructures*, 1(2/3):247–257, 2005.

[MF99] J. McDermott and C. Fox. Using abuse case models for security requirements analysis. In *ACSAC '99: Proceedings of the 15th Annual Computer Security Applications Conference*, pages 55–64, 6-10 Dec. 1999.

[MH07] J. R. W. Merrick and J. R. Harrald. Making decisions about security in US ports and waterways. *Interfaces*, 37:240–252, 2007.

[Mül05] M. Müller. *Workflow-based Integration: Grundlagen, Technologien, Management.* Springer, 2005.

[Moy05] D. Moynihan. Business process modeling: A proven methodology for enterprise integration. CIO Newsletter, September 2005.

[MPD92] R. J. Mayer, M. K. Painter, and P. S. DeWitte. Idef family of methods for concurrent engineering and business re-engineering applications. Technical report, Knowledge Based Systems, 1992.

[MV00] D. Moldt and R. Valk. Object oriented petri nets in business process modeling. In *Business Process Management, Models, Techniques, and Empirical Studies*, pages 254–273, London, UK, 2000. Springer.

[Neu07] T. Neubauer. *Business Process Based Valuation and Selection of IT Investments, Development and Implementation of a Method for the Interactive Selection of IT Investments under Multiple Objectives.* PhD thesis, Vienna University of Technology, Institute of Software Technology and Interactive Systems, October 2007.

[NH07a] T. Neubauer and J. Heurix. Business process driven security safeguard selection with respect to multiple objectives. Technical Report SBA-07-11-15, Secure Business Austria, November 2007.

[NH07b] T. Neubauer and J. Heurix. Defining secure business processes with respect to multiple objectives: A case study. Technical Report SBA-07-11-10, Secure Business Austria, November 2007.

[NH07c] T. Neubauer and J. Heurix. An evaluation of concepts for information security safeguard selection. Technical Report SBA-07-11-20, Secure Business Austria, November 2007.

[NH07d] T. Neubauer and J. Heurix. Multiobjective decision support for defining secure business processes. In *The Ninth International Conference on Information Integration and Web-based Applications Services, OCG, 2007*, number SBA-07-06-01, April 2007.

[NH08] T. Neubauer and J. Heurix. Defining secure business processes with respect to multiple objectives. Technical report, Secure Business Austria, 2008.

[NK06] S. Nevo and H. Kim. How to compare and analyse risks of internet voting versus other modes of voting. *Electronic Government*, 3(1):105–112, 2006.

[NKB06] T. Neubauer, M. Klemen, and S. Biffl. Secure business process management: a roadmap. In *ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security*, page 8, 20-22 April 2006.

[Nor00] O. S. Noran. Business modelling: Uml vs. idef. Technical report, Griffith University School of Computing and Information Technology, 2000.

[NS87] J. D. Newton and C. A. Snyder. Risk analysis for computerized information systems. Southern Management Association, 1987.

[NS07a] T. Neubauer and C. Stummer. Extending business process management to determine efficient it investments. In *SAC '07: Proceedings of the 2007 ACM symposium on Applied computing*, pages 1250–1256, New York, NY, USA, 2007. ACM Press.

[NS07b] T. Neubauer and C. Stummer. Interactive decision support for multiobjective cots selection. In *HICSS 2007: Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, 2007.

[NSW06] T. Neubauer, C. Stummer, and E. Weippl. Workshop-based multiobjective security safeguard selection. In *ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security*, page 8, 20-22 April 2006.

[OMG99] OMG. Requirements for uml profiles. Technical report, OMG - Analysis and Design Platform Task Force, December 1999.

[OMG06] OMG. Business process modeling notation specification. Final adopted specification, Object Management Group, February 2006.

[OMG07a] OMG. Unified modeling language: Infrastructure. Technical specification, Object Management Group, 2007.

[OMG07b] OMG. Unified modeling language: Superstructure. Technical specification, Object Management Group, February 2007.

[Oul95] M. A. Ould. *Business Processes: Modelling and Analysis for Re-engineering and Improvement.* John Wiley & Sons, 1995.

[Pel05] T. R. Peltier. *Information Security Risk Analysis.* Auerbach Publications, 2nd edition, 2005.

[Pfl97] C. P. Pfleeger. The fundamentals of information security. *IEEE Software*, 14(1):15–16,60, 1997.

[Pic89] R. Pickard. Computer crime. *Information Center*, 5(9):18–27, 1989.

[Pid03] P. Pidd. *Tools for Thinking: Modelling in Management Science.* John Wiley & Sons, 2nd edition edition, 2003.

[RFMP06] A. Rodriguez, E. Fernandez-Medina, and M. Piattini. Security requirements with a uml 2 profile. In *Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)*, 2006.

[Röh02] S. Röhrig. Using process models to analyze health care security requirements. In *International Conference Advances in Infrastructure for e-Business, e-Education, e-Science, and e-Medicine on the Internet*, Italy, January 2002.

[Röh03] S. Röhrig. *Using Process Models to Analyse IT Security Requirements.* Phd thesis, University of Zurich, March 2003.

[RHP99] A. Röhm, G. Herrmann, and G. Pernul. A language for modelling secure businesstransactions. In *Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC'99)*, volume 22-31. IEEE Computer Society Press, 1999.

[RK04] S. Röhrig and K. Knorr. Security analysis of electronic business processes. *Electronic Commerce Research*, 4:59–81, 2004.

[RSC91] R. K. Rainer, C. A. Snyder, and H. H. Carr. Risk analysis for information technology. *J. Manage. Inf. Syst.*, 8(1):129–147, 1991.

[Saa80] T. L. Saaty. *The Analytic Hierarchy Process.* McGraw-Hill, 1980.

[Saa90] T. L. Saaty. How to make a decision: The analytic hierarchy process. *European Journal of Operational Research*, 48:9–26, 1990.

[Saa94] T. L. Saaty. How to make a decision: The analytic hierarchy process. *Interfaces*, 24(6):19–44, 1994.

[Sad04] A. Sademies. Process approach to information security metrics in finnish industry and state institutions. In *VTT Publications 544*. 2004.

[San03] R. Sandhu. Good-enough security. *IEEE Internet Computing*, 7(1):66–68, 2003.

[SBP04] J. D. L. Silva, E. K. Burke, and S. Petrovic. An introduction to multiobjective metaheuristics for scheduling and timetabling. In *Metaheuristics for Multiobjective Optimisation.* Springer, 2004.

[Sch92] A. W. Scheer. *Architecture of integrated information systems.* Springer, 1992.

[Sch99] A. W. Scheer. *ARIS - Business Process Frameworks.* Springer, 3rd edition edition, 1999.

[Sch00] A. W. Scheer. *ARIS - Business Process Modeling.* Springer, 3rd edition edition, 2000.

[SCS+03] N. Stathiakis, C. Chronaki, E. Skipenes, E. Henriksen, E. Charalambous, A. Sykianakis, G. Vrouchos, N. Antonakis, M. Tsiknakis, and S. Orphanoudakis. Risk assessment of a cardiology ehealth service in hygeianet. In *Proc. Computers in Cardiology (CIC'2003)*, 2003.

[SdBF+02] K.l Stolen, F. den Braber, R. Fredriksen, B. A. Gran, S. Houmb, M. S. Lund, Y. C. Stamatiou, and J. O. Aagedal. Model-based risk assessment - the coras approach. In *Proc. Norsk Informatikkkonferanse (NIK'2002)*, pages 239–249, 2002.

[SGF02] G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems. Nist special publication (sp 800-30), National Institute of Standards and Technology, 2002.

[SH00] A. W. Scheer and F. Habermann. Enterprise resource planning: making erp a success. *Communications of the ACM*, 43(4):57–61, 2000.

[SH03] B. Suh and I. Han. The is risk analysis based on a business model. *Inf. Manage.*, 41(2):149–158, 2003.

[SHF01] G. Stoneburner, C. Hayden, and A. Feringa. Engineering principles for information technology security. Technical report, National Institute of Standards and Technology, 2001.

[Shi00] R. Shirey. Internet security glossary - request for comments: 2828. Online at `http://www.faqs.org/rfcs/rfc2828.html`, May 2000.

[SHL$^+$02] Y. C. Stamatiou, E. Henriksen, M. S. Lund, E. Mantzouranis, M. Psarros, E. Skipenes, N. Stathiakos, and K. Stolen. Experiences from using model-based risk assessment to evaluate the security of a telemedicine application. In *Proc. Telemedicine in Care Delivery (TICD'2002)*, pages 115–119, 2002.

[Smi93] M. Smith. *Commonsense Computer Security - your practical guide to inforation security*. McGraw-Hill, London, 1993.

[SMS01] H. A. Smith, J. D. McKeen, and D. S. Staples. Risk management in information systems: problems and potential. *Communications of the Association for Information Systems (AIS)*, 7, 2001.

[SO00] G. Sindre and A.L. Opdahl. Eliciting security requirements by misuse cases. In *TOOLS-Pacific 2000: Proceedings of the 37th International Conference onTechnology of Object-Oriented Languages and Systems*, pages 120–131, 20-23 Nov. 2000.

[Soo00] K. J. SooHoo. How much is enough? a risk-management approach to computer security. Technical report, Consortium for Research on Information Security and Policy (CRISP), June 2000.

[SSH$^+$03] Y. Stamatiou, E. Skipenes, E. Henriksen, N. Stathiakis, A. Sikianakis, E. Charalambous, N. Antonakis, K.l Stolen, F. den Braber, M. S. Lund, K. Papadaki, and G. Valvis. The coras approach for model-based risk management applied to a telemedicine service. In *Proc. Medical Informatics Europe (MIE'2003)*, pages 206–211, 2003.

[SVC$^+$01] P. Sinogas, A. Vasconcelos, A. Caetano, J. Neves, R. Mendes, and J. Tribolet. Business processes extensions to uml profile for business modeling. In *Proceedings of the International Conference on Enterprise Information Systems*, 2001.

[SW94] R. A. Snowdon and B. C. Warboys. An introduction to process-centred environments. In A. Finkelstein, J. Kramer, and B. Nuseibeh, editors, *Software Process Modelling and Technology*, pages 1–8. John Wiley & Sons Inc, 1994.

[SY98] P. Sen and J. B. Yang. *Multiple Criteria Decision Support in Engineering Design.* Springer, 1998.

[TMW96] E. Turban, E. McLean, and J. Wetherbe. *Information Technology for Management: Improving Quality and Productivity.* John Wiley & Sons, 1996.

[TS00] S. Teufel and T. Schlienger. Informationssicherheit - wege zur kontrollierten unsicherheit. *HMD - Praxis Wirtschaftsinform*, 216:18–31, 2000.

[VE03] H. Venter and J. Eloff. A taxonomy of information security technologies. *Computers and Security*, 22:299–307, May 2003.

[Vid04] S. Vidalis. Critical discussion of risk and threat analysis methods and methodologies. Soc technical report, University of Glamorgan, July 2004.

[VK06] O. S. Vaidya and S. Kumar. Analytic hierarchy process: An overview of applications. *European Journal of Operations Research*, 169:1–29, 2006.

[VP07] VP. Visual paradigm - uml 2 diagrams. Online at http://www.visual-paradigm.com/VPGallery/diagrams/index.html, Access in May 2007.

[WFM95] WFMC. Workflow management coalition - the workflow reference model. Technical Report TC00-1003, Workflow Management Coalition, 1995.

[WFM98] WFMC. Interface 1: Process definition interchange - process model. Technical report, Workflow Management Coalition, 1998.

[WFM99] WFMC. Workflow management coalition - terminology & glossary. Technical Report WfMC-TC-1011, Workflow Management Coalition, 1999.

[WvdAV04] M. Weske, W. M. P. van der Aalst, and H. M. W. Verbeek. Advances in business process management. *Data Knowledge & Engineering*, 50(1):1–8, 2004.

[Zai97] M. Zairi. Business process management: a boundaryless approach to modern competitiveness. *Business Process Management*, 3(1):64–80, 1997.

[ZLB04] E. Zitzler, M. Laumanns, and S. Bleuler. A tutorial on evolutionary multiobjective optimization. In *Metaheuristics for Multiobjective Optimisation*. Springer, 2004.

[zMR05] M. zur Muehlen and M. Rosemann. Integrating risks in business process models. In *Proceedings of the 16th Australasian Conference on Information Systems*, 2005.